IN5540 - Privacy by Design

Tanusan Rajmohan - tanusanr@ifi.uio.no

UNIVERSITY OF OSLO

Autumn 2019

Contents

Learning outcome

After completing this course, you will:

- have knowledge of basic legal privacy concepts and data protection regulations
- have knowledge of security and privacy enhancing technologies
- have knowledge of concepts of privacy by design and privacy impact assessment
- have knowledge of principles of architectural tactics for privacy and privacy patterns
- be able to map legal privacy principles to technical privacy concepts
- be able to relate security and privacy goals to mechanisms and technologies
- be able to apply privacy by design and perform privacy impact assessments
- be able to apply appropriate architectural tactics for privacy and privacy patterns

1 Lecture 1: Introduction lecture

1.1 Course Introduction

- What is privacy? Why privacy?
- Privacy issues in information technology
- Some examples of data breaches
- Case study: personal data extraction of popular apps

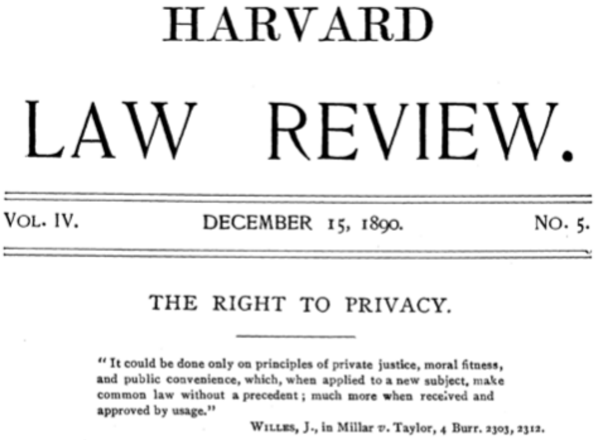
1.2 What is privacy?

Privacy is expressed in relationships to others.

1.2.1 History

- "Right to be left alone"
- Warren/Brandeis in 1890 in USA.
- Reaction to paparazzi intrusions in new media (press photography)

"**Recent inventions and business methods call attention to the next step which must be taken for the protection of the person**, and for securing to the individual what Judge Cooley calls the right "to be left alone" Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the housetops."
Warren/Brandeis, **The Right to Privacy**, 4 Harvard L.R. 193 (Dec. 15, 1890)



HARVARD

LAW REVIEW.

VOL. IV. DECEMBER 15, 1890. NO. 5.

THE RIGHT TO PRIVACY.

" It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent ; much more when received and approved by usage."

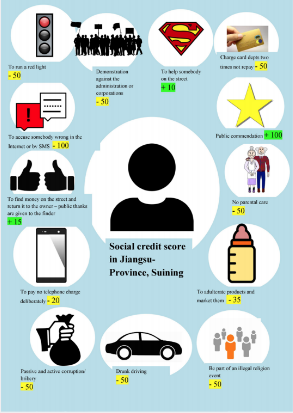
WILLES, J., in Millar *v.* Taylor, 4 Burr. 2303, 2312.

1.2.2 Declaration of Human Rights, 1948

"No one shall be subjected to arbitrary interference with his **privacy**, family, home or **correspondence** nor to attacks upon his **honor** and **reputation**. Everyone has the right to the **protection** of the law **against such interference** or attacks." (Article 12, The Universal Declaration of Human Rights, 1948)

- **Bloustein (1964)** “inviolate personality” is the social value protected by privacy. “A man whose ... conversation may be overheard at the will of another, whose marital and familial intimacies may be overseen at the will of another, is less of a man, has less human dignity, on that account.”
- **Westin (1967)** defines privacy as (the) claim of individuals . . . to determine for themselves when, how, and to what extent information about them is communicated to others.
- **Breckenridge (1970)**. Privacy is the rightful claim of the individual to determine the extent to which he wishes to share of himself with others and his control over the time, place and circumstances to communicate with others.
- **Fried (1968/1984)** Privacy is the control we have over information about ourselves.
- **Altman (1975)** ....boundary control mechanism for limiting information flows.... Primary (has control)...semi- public (moderate control) ...public (no control).
- **Posner (1978)** ...withholding and concealment of information... ...economic interest..... thought of as property that can be bought and sold.
- **Gavison (1980)** Privacy is limitation of others’ access” to information about individuals. What constitute limited access is the three independent and irreducible elements: secrecy, anonymity, and solitude.
- **Schoeman (1984)** three categories: (i) privacy as a claim, entitlement, or right; (ii) privacy as a measure of control over information, intimacies, or access; and (iii) privacy as a state or condition of limited access to a person.

1.2.3 It’s not just the businesses...


To run a red light - 50
Demonstration against the administration or corporations - 50
To help somebody on the street + 10
Charge card depts two times not repay - 50
To accuse somebody wrong in the Internet or by SMS - 100
Public commendation + 100
To find money on the street and return it to the owner – public thanks are given to the finder + 15
Social credit score in Jiangsu-Province, Suining
No parental care - 50
To pay no telephone charge deliberately - 20
To adulterate products and market them - 35
Passive and active corruption/ bribery - 50
Drunk driving - 50
Be part of an illegal religion event - 50

Data Scores as Governance: Investigating uses of citizen scoring in public services

Project Report

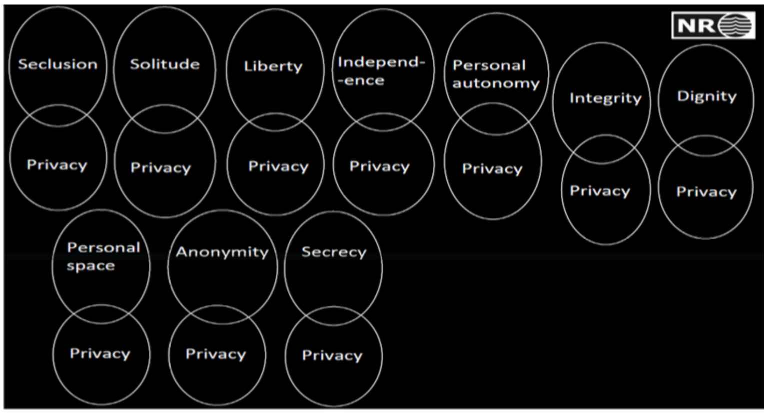
Lina Dencik, Arne Hintz, Joanna Redden & Harry Warne

Data Justice Lab

Cardiff University Prifysgol Caerdydd

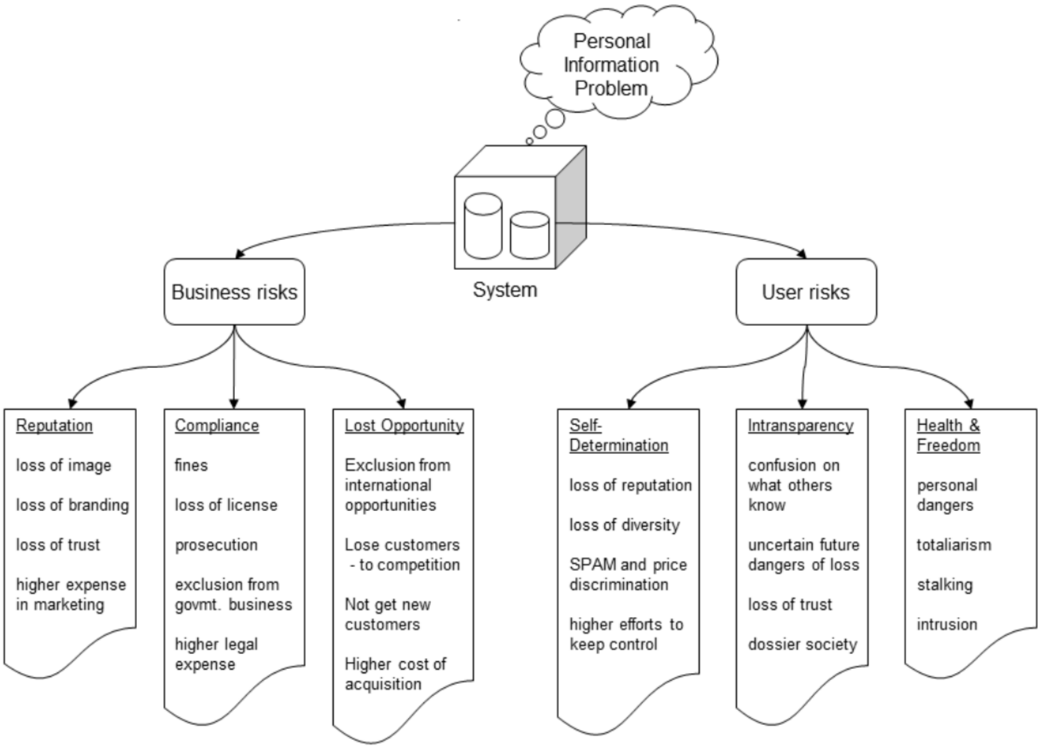
OPEN SOCIETY FOUNDATIONS

- Health scoring?
- Earning of pension points by conforming to dominant work ideology?
- School grades determine university acess?
- Parental leave – when conforming to gender policy metrics?
- GPS-based road toll to control traffic patterns?



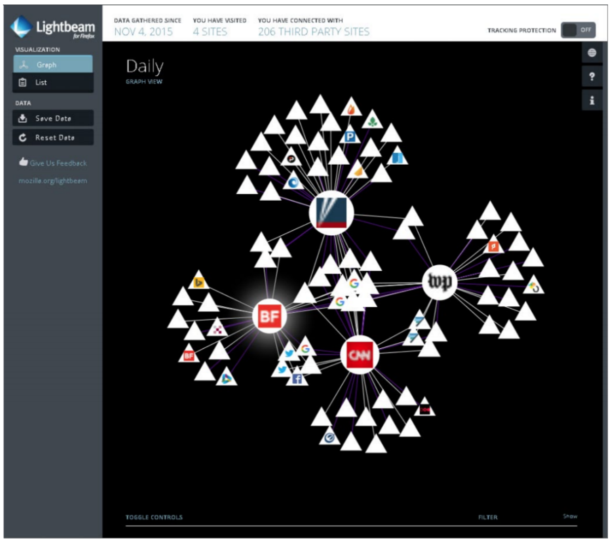
1.3 Privacy issues in information technology

1.3.1 Duality of privacy risks

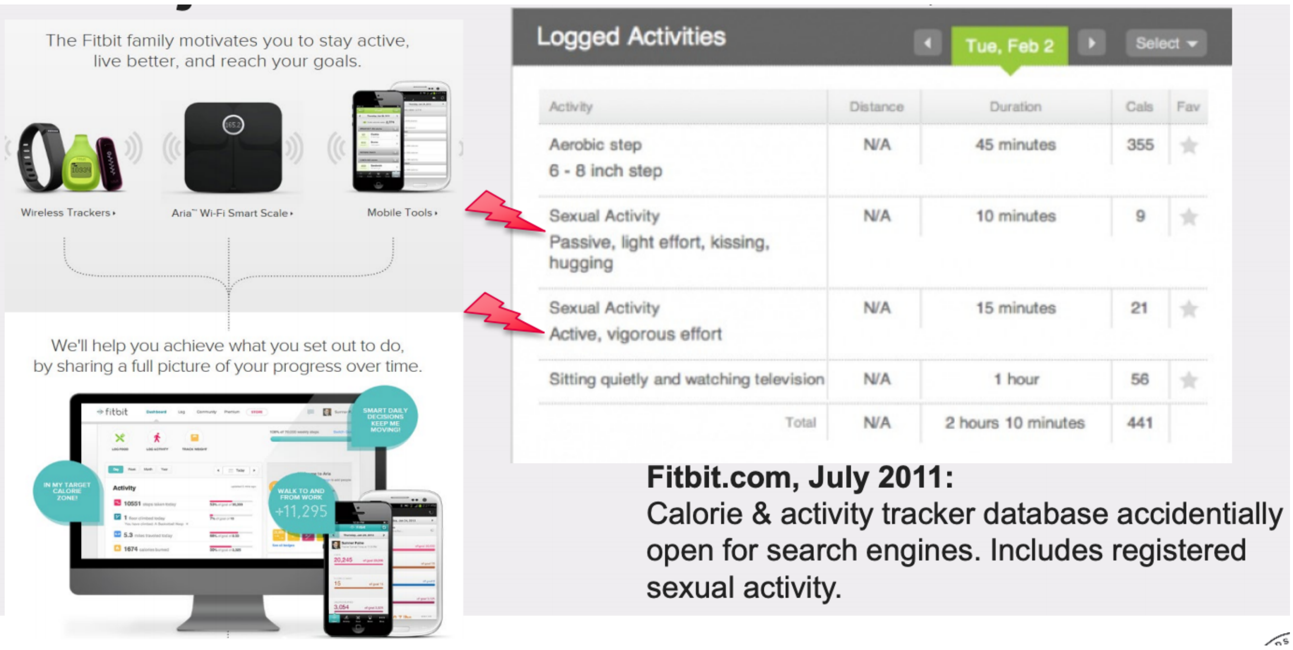


1.3.2 3rd party tracking

A screenshot of **Lightbeam**, an add-on for Firefox that lets you see what third party sites you've connected to during your web browsing. After opening the frontpages of Fox News, Buzzfeed, CNN, and The Washington Post, we've been connected to 206 third party sites



On-line journals for exercise, diet


The Fitbit family motivates you to stay active, live better, and reach your goals.
Wireless Trackers ›
Aria™ Wi-Fi Smart Scale ›
Mobile Tools ›
We'll help you achieve what you set out to do, by sharing a full picture of your progress over time.
IN MY TARGET CALORIE ZONE!
SMART DAILY DECISIONS KEEP ME MOVING!
WALK TO AND FROM WORK
+11,295

Logged Activities

Tue, Feb 2

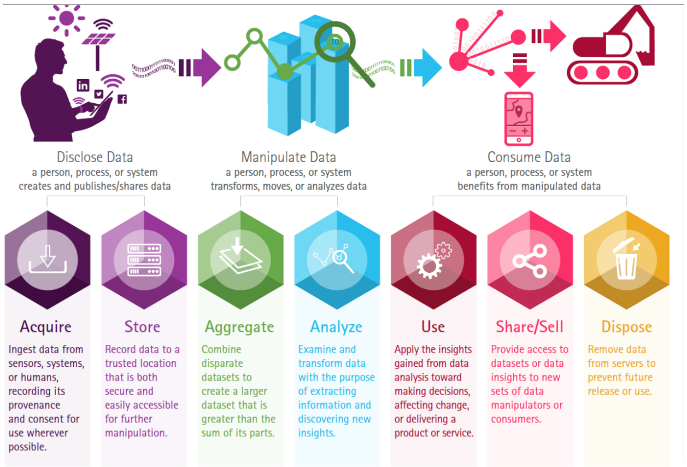
Select

Activity	Distance	Duration	Cals	Fav
Aerobic step 6 - 8 inch step	N/A	45 minutes	355	★
Sexual Activity Passive, light effort, kissing, hugging	N/A	10 minutes	9	★
Sexual Activity Active, vigorous effort	N/A	15 minutes	21	★
Sitting quietly and watching television	N/A	1 hour	56	★
Total	N/A	2 hours 10 minutes	441	

Fitbit.com, July 2011:
Calorie & activity tracker database accidentally open for search engines. Includes registered sexual activity.

1.3.3 Data is the new oil ... what about the oil spills?

- Massive data collection, analysis and distribution capacity
- "Big Data" promises near-magic self learning, knowledge-discovering and artificially intelligent computers – if they just get fed enough information.
- Data leakage, data sabotage, espionage and poor data quality are serious threats
- Hard to revert a "data spill" once data has leaked, been stolen or published.
- Potential for personal compromise as well as a threat to IT product vendors – or endangering national security and sovereignty



Disclose Data
a person, process, or system creates and publishes/shares data

Manipulate Data
a person, process, or system transforms, moves, or analyzes data

Consume Data
a person, process, or system benefits from manipulated data

Acquire
Ingest data from sensors, systems, or humans, recording its provenance and consent for use wherever possible.

Store
Record data to a trusted location that is both secure and easily accessible for further manipulation.

Aggregate
Combine disparate datasets to create a larger dataset that is greater than the sum of its parts.

Analyze
Examine and transform data with the purpose of extracting information and discovering new insights.

Use
Apply the insights gained from data analysis toward making decisions, affecting change, or delivering a product or service.

Share/Sell
Provide access to datasets or data insights to new sets of data manipulators or consumers.

Dispose
Remove data from servers to prevent future release or use.

1.3.4 ENISA PIA Impact Levels

The European Union Agency For Network and Information Security (ENISA) has published guidelines for privacy risk assessment for Small and Medium Enterprises that contain guidance on privacy impact assessment focused on individual data subjects in chapter 3 on page 19. There, four levels of privacy impact are defined:

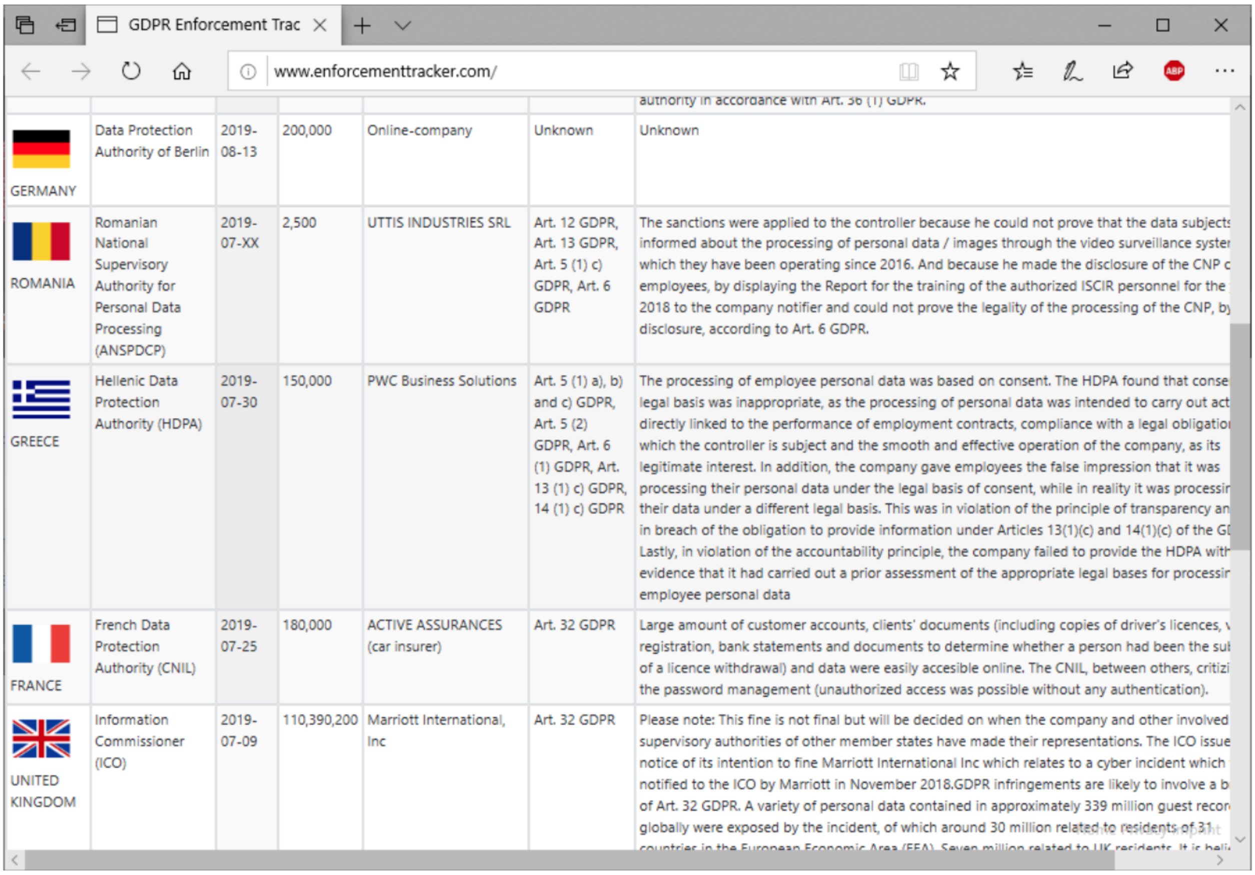
LEVEL OF IMPACT	DESCRIPTION
Low	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc.).
Very high	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

1.4 Data breaches

What happens? Who gets fined? What DO IT-systems with our data?

The World's Biggest Data Breaches

$http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/$



						authority in accordance with Art. 36 (1) GDPR.
GERMANY	Data Protection Authority of Berlin	2019-08-13	200,000	Online-company	Unknown	Unknown
ROMANIA	Romanian National Supervisory Authority for Personal Data Processing (ANSPDCP)	2019-07-XX	2,500	UTTIS INDUSTRIES SRL	Art. 12 GDPR, Art. 13 GDPR, Art. 5 (1) c) GDPR, Art. 6 GDPR	The sanctions were applied to the controller because he could not prove that the data subjects informed about the processing of personal data / images through the video surveillance syster which they have been operating since 2016. And because he made the disclosure of the CNP c employees, by displaying the Report for the training of the authorized ISCIR personnel for the 2018 to the company notifier and could not prove the legality of the processing of the CNP, by disclosure, according to Art. 6 GDPR.
GREECE	Hellenic Data Protection Authority (HDPA)	2019-07-30	150,000	PWC Business Solutions	Art. 5 (1) a), b) and c) GDPR, Art. 5 (2) GDPR, Art. 6 (1) GDPR, Art. 13 (1) c) GDPR, 14 (1) c) GDPR	The processing of employee personal data was based on consent. The HDPA found that conse legal basis was inappropriate, as the processing of personal data was intended to carry out act directly linked to the performance of employment contracts, compliance with a legal obligatio which the controller is subject and the smooth and effective operation of the company, as its legitimate interest. In addition, the company gave employees the false impression that it was processing their personal data under the legal basis of consent, while in reality it was processin their data under a different legal basis. This was in violation of the principle of transparency an in breach of the obligation to provide information under Articles 13(1)(c) and 14(1)(c) of the GI Lastly, in violation of the accountability principle, the company failed to provide the HDPA with evidence that it had carried out a prior assessment of the appropriate legal bases for processin employee personal data
FRANCE	French Data Protection Authority (CNIL)	2019-07-25	180,000	ACTIVE ASSURANCES (car insurer)	Art. 32 GDPR	Large amount of customer accounts, clients' documents (including copies of driver's licences, v registration, bank statements and documents to determine whether a person had been the sul of a licence withdrawal) and data were easily accesible online. The CNIL, between others, critizi the password management (unauthorized access was possible without any authentication).
UNITED KINGDOM	Information Commissioner (ICO)	2019-07-09	110,390,200	Marriott International, Inc	Art. 32 GDPR	Please note: This fine is not final but will be decided on when the company and other involved supervisory authorities of other member states have made their representations. The ICO issue notice of its intention to fine Marriott International Inc which relates to a cyber incident which notified to the ICO by Marriott in November 2018.GDPR infringements are likely to involve a b of Art. 32 GDPR. A variety of personal data contained in approximately 339 million guest recor globally were exposed by the incident, of which around 30 million related to residents of 31 countries in the European Economic Area (EEA). Seven million related to UK residents. It is beli

Figure 1: $http://www.enforcementtracker.com/$

2 Lecture 2: Privacy / GDPR

2.1 How privacy is determining our lives

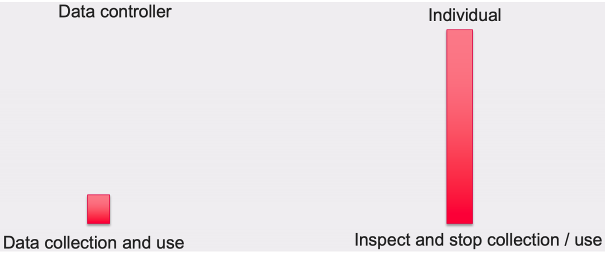
There are obvious "use cases" for privacy:

- Voting secrecy is a strong foundation for democracy.
- Protection against discrimination on grounds of political opinion, relationships, religion and philosophy.
- Enables personal freedom and independence in thinking and development

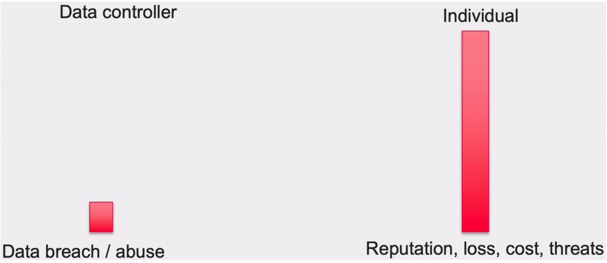
Access to - and control over - personal data does create power over individuals. Lets' explore this power relationship!

2.2 Fairness & privacy

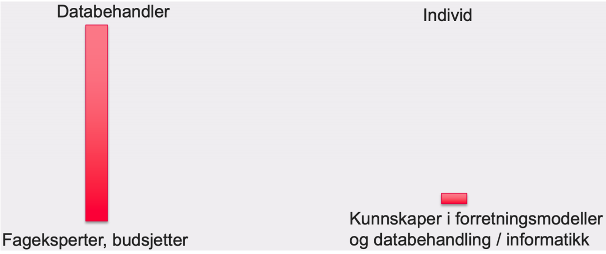
2.2.1 Asymmetric cost



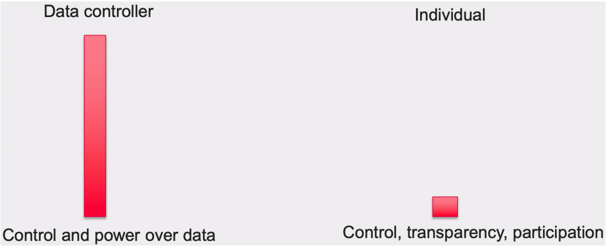
2.2.2 Asymmetric risk



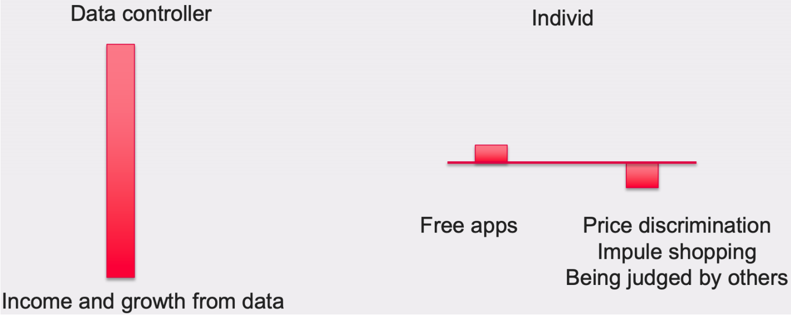
2.2.3 Asymmetric knowledge



2.2.4 Control and freedom

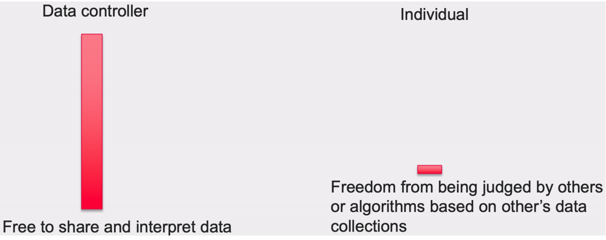


2.2.5 Asymmetric knowledge

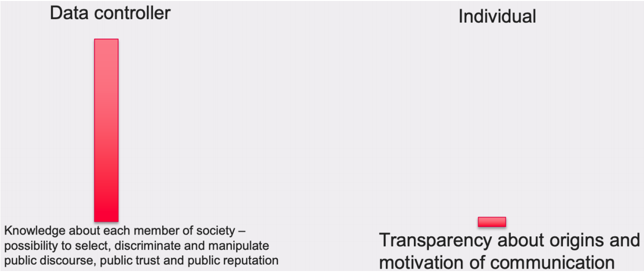


2.3 Society and privacy

2.3.1 Control and freedom



2.3.2 Attack on sovereignity



2.4 Privacy Principles

Trade agreements cover data exchange, too!

- Software gets traded or hosted across borders.
- Therefore: international agreements, laws and standards about personal data handling across borders.

Historically:

- Local legislation in individual countries from the 1970ies (USA, France, Germany)
- EU started harmonizing, resulting in first EU directive
- Updated with EU regulation GDPR (and soon will be enriched with EU e-Privacy regulation)
- Other regions in the world have other privacy regulation. Special rules apply for specific sectors such as health or finance.

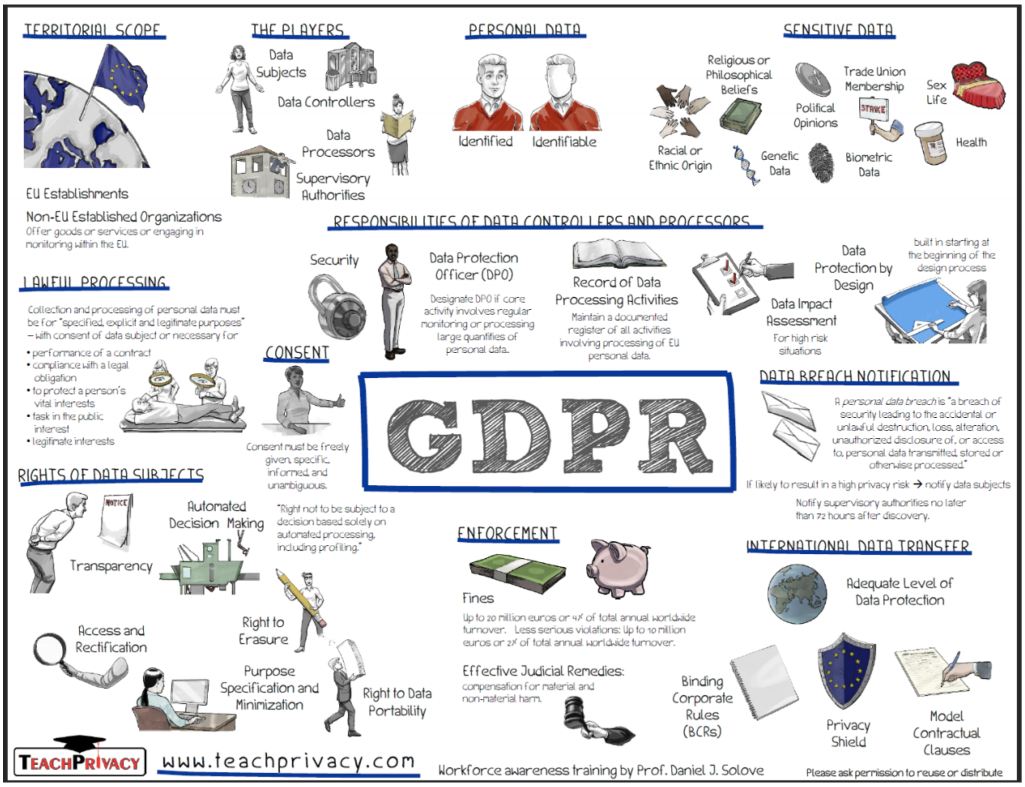
In EU/EFTA, GDPR gets ”translated” into national laws, e.g. **Personvernsloven** in Norway.

2.4.1 Basic Privacy Principles

(part of OECD Privacy Guidelines & most Privacy/Data Protection Laws)

- **Lawfullness of processing**, e.g. by **Informed Consent** (c.f. OECD Collection Limitation Principle)
- **Data Minimisation** & **Avoidance** (c.f. OECD Data Quality Principle)
  - Data should be adequate, relevant and not exessive
  - Minimisation of data collection, use, sharing, linkability, retention
- **Purpose Specification** & **Purpose Binding** (c.f. OECD Purpose Specification Principle & Use Limitation Principle)
  - ”Non-sensitive” data do not exist !
- Examples of Purpose Misuse ("function creep"):
  - Lidl Video Monitoring Scandal (2006) $https://www.theguardian.com/world/2008/mar/27/germany.supermarkets$
  - Loyality Card Data use against customer interests
- **Transparency** and **Intervenability** (c.f. OECD Openness Principle & Individual Participation Principle)
- Appropriate **Security** (c.f. OECD Security Safeguards Principle)
- **Accountability** (c.f. OECD Accountability Principle)

2.5 GDPR Whiteboard - Dan Solove



Offer goods or services or engaging in monitoring within the EU.

Collection and processing of personal data must be for "specified, explicit and legitimate purposes" – with consent of data subject or necessary for

- performance of a contract
- compliance with a legal obligation
- to protect a person's vital interests
- task in the public interest
- legitimate interests

RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS
Security
Data Protection Officer (DPO)

Designate DPO if core activity involves regular monitoring or processing large quantities of personal data.

Maintain a documented register of all activities involving processing of EU personal data.

Data Impact Assessment
For high risk situations
Data Protection by Design
built in starting at the beginning of the design process
CONSENT

Consent must be freely given, specific, informed, and unambiguous.

A *personal data breach* is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

If likely to result in a high privacy risk → notify data subjects

Notify supervisory authorities no later than 72 hours after discovery.

"Right not to be subject to a decision based solely on automated processing, including profiling."

Access and Rectification
Right to Erasure
Purpose Specification and Minimization
Right to Data Portability
ENFORCEMENT
Fines

Up to 20 million euros or 4% of total annual worldwide turnover. Less serious violations: Up to 10 million euros or 2% of total annual worldwide turnover.

compensation for material and non-material harm.

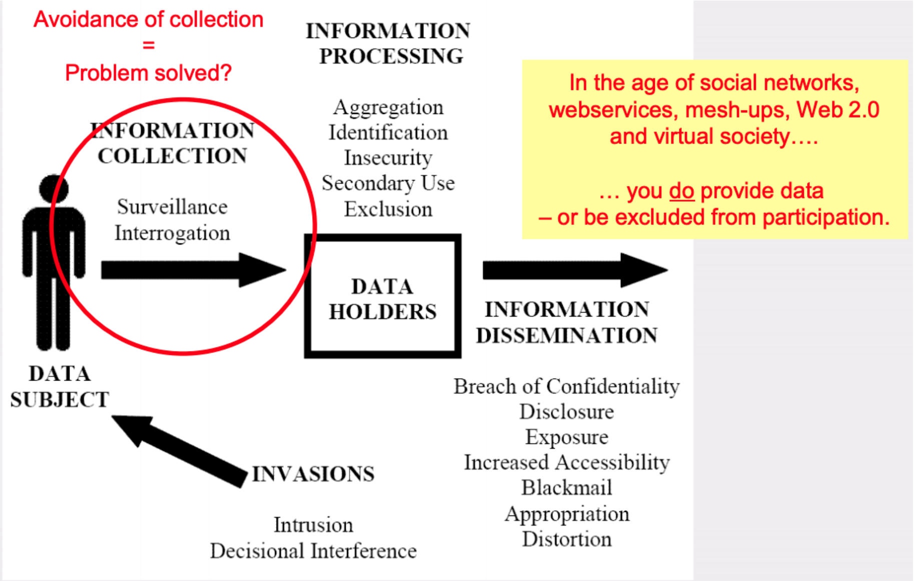
INTERNATIONAL DATA TRANSFER
Adequate Level of Data Protection
Binding Corporate Rules (BCRs)
Privacy Shield
Model Contractual Clauses
TEACHPRIVACY
www.teachprivacy.com

Workforce awareness training by Prof. Daniel J. Solove

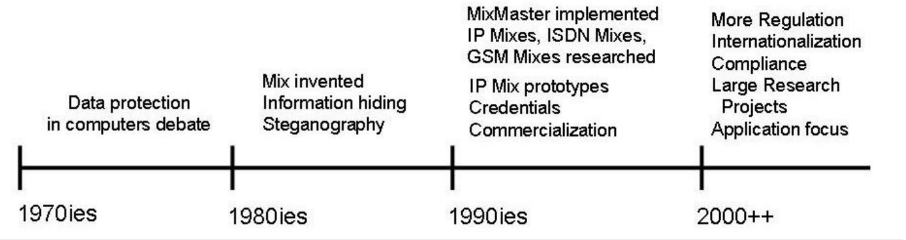
Please ask permission to reuse or distribute

3 Lecture 3: Privacy Enhancing Technology

3.1 Solove's privacy threat taxonomy

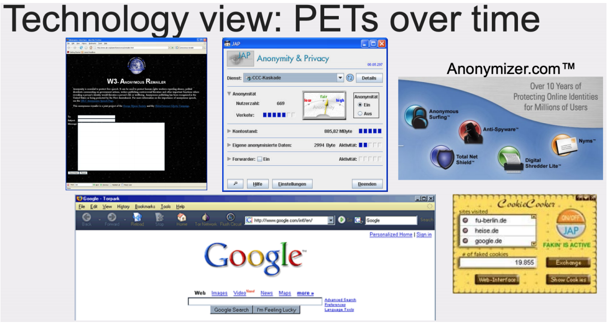


3.2 A brief history of PET

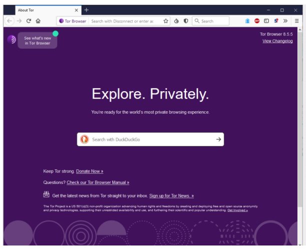


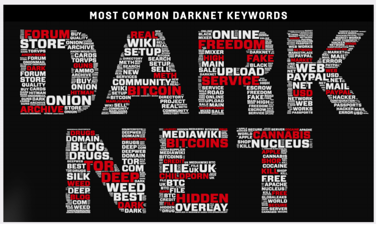
- PET development inspired by the legal perspective on basic human rights.
- PET research focused on information hiding & control
- Technology-centric approach

But there is a lack of deployed PETs in the ”real world”. Why?



Technology view: PETs over time





3.3 Identity, Identification, Anonymity

3.3.1 What is an e-ID?

- ...is a portion of digital data together with algorithms in hard- or software that have the purpose of convincing a computer that a particular, possibly privileged, person is using the computer.
- e-ID can be based on official documents, e.g. passports
- Many e-Ids are attached to "soft identities" such as e-mail addresses, user pseudonyms, ...
- E-ID is used for many different purposes.
- E-ID is possibly attached to a communication channel.
- E-ID and its attachment to real identity can be chosen (free choice of pseudonym and attributes in OpenID), or mandatory (government e-ID). E-ID enables aggregation of personal profiles with additional attributes.

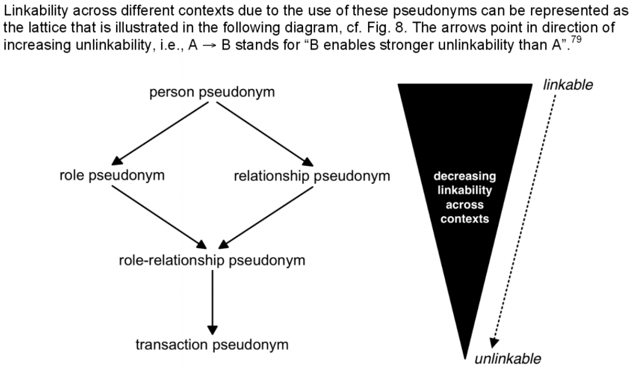
3.3.2 Control over e-ID

- Categories of identity
  - "Me-Identity": What I define as identity
  - "Our-Identity": What others and I define as identity
  - "Their-Identity": What others define as my identity
- Purposes of Identity Management
  - Identification
  - Managing attributes (database)
  - Privacy-enhanced(self-)management

3.3.3 Basic Identity-based Transactions

- **Identification**
  Who is the user – used on logon or database lookup
- **Authentication**
  Is this the real user? Please provide evidence!
- **Authorization and non-repudiation**
  Authorization of documents or transaction with e-ID and most often with digital signature based on e-ID. Generates non-repudiation and receipts.
- Pseudonyms can be used for many such purposes, too. This is called "**privacy- enhancing identity management**" by Pfitzmann and Hansen.

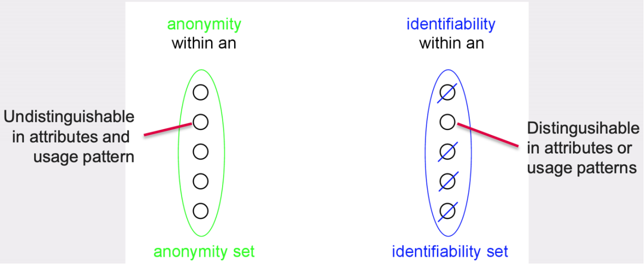
3.3.4 Degrees of anonymity and linkability



Linkability across different contexts due to the use of these pseudonyms can be represented as the lattice that is illustrated in the following diagram, cf. Fig. 8. The arrows point in direction of increasing unlinkability, i.e., A → B stands for "B enables stronger unlinkability than A".[79]

3.3.5 Identifiability

Identifiability of a subject from an attacker's perspective means that the attacker can sufficiently identify the subject within a set of subjects, the identifiability set [Pfitzmann-Hansen]


anonymity
within an
Undistinguishable in attributes and usage pattern
anonymity set
identifiability
within an
Distingusihable in attributes or usage patterns
identifiability set

3.3.6 Synthetic identities

- Identifiers can be "created" from observed data, e.g.:
  - IP addresses
  - Combined data (e.g. user accounts and location data)
  - By data mining for behavioral patterns
  - From observing biometric signals (e.g. voice)
- Such "synthetic" partial identities can appear beyond the control of the data subject, and may get used by the owners of "Big Data" collections for analysis, decision- making or further observation of data subjects. They can be recognized, e.g. from mobile phone movement patterns.
- Eventually, they can turn into person-related data (e.g. by observing the place of home or place of work frequently visited in a location track).

3.3.7 Important concepts - remember!

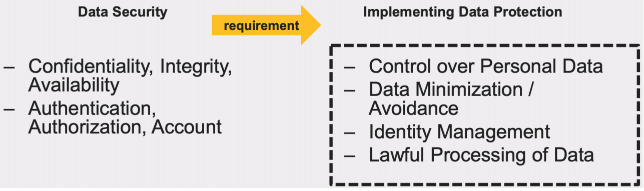
- Unobservability - ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used.
- Partial identities
- Anonymity & Pseudonymity (Pseudonymity is the near-anonymous state in which a user has a consistent identifier that is not their real name: a pseudonym.)
- Unlinkability

3.4 Security Technologies

Have objectives:

- Confidentiality
- Integrity
- Availability
- Authentication
- Authorization
- Accounting

3.4.1 Technical Means for Securing Data



Data Security

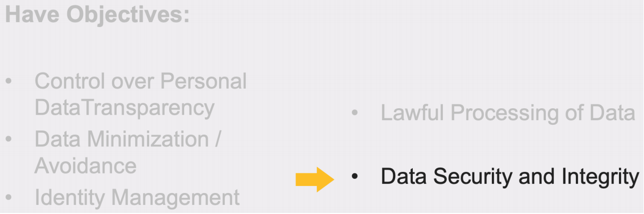
– Confidentiality, Integrity, Availability
– Authentication, Authorization, Account

requirement

Implementing Data Protection

– Control over Personal Data
– Data Minimization / Avoidance
– Identity Management
– Lawful Processing of Data

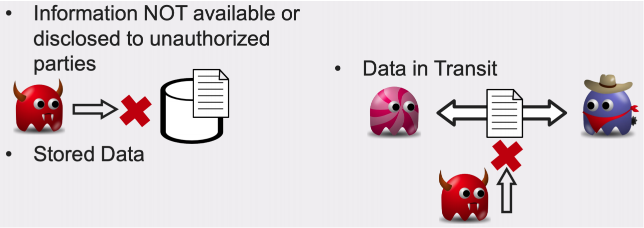
3.4.2 Privacy Enhancing Technologies



Have Objectives:

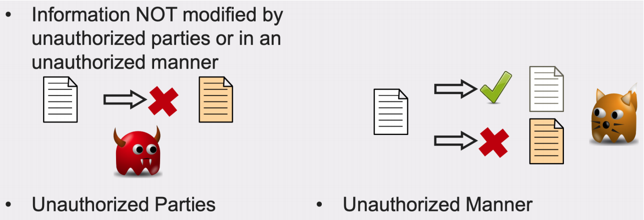
- Control over Personal DataTransparency
- Data Minimization / Avoidance
- Identity Management
- Lawful Processing of Data
- Data Security and Integrity

3.4.3 Confidentiality



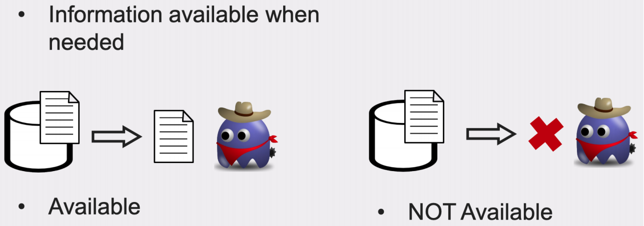
- Information NOT available or disclosed to unauthorized parties
- Stored Data
- Data in Transit

3.4.4 Integrity



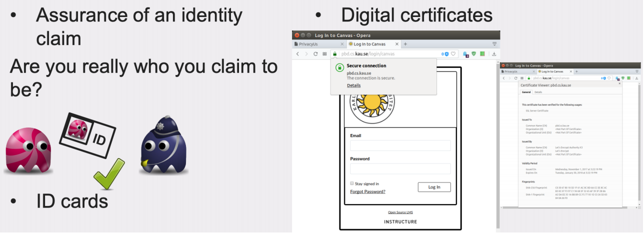
- Information NOT modified by unauthorized parties or in an unauthorized manner
- Unauthorized Parties
- Unauthorized Manner

3.4.5 Availability



- Information available when needed
- Available
- NOT Available

3.4.6 Authentication

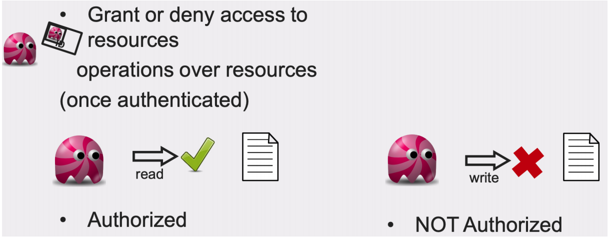


- Assurance of an identity claim

Are you really who you claim to be?

- ID cards
- Digital certificates

3.4.7 Authorization



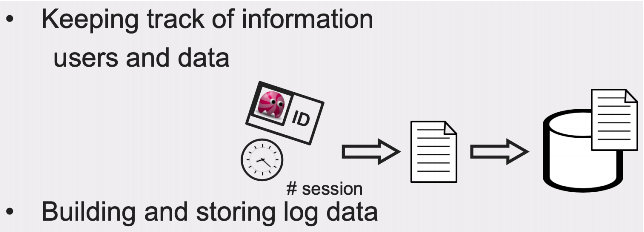
- Grant or deny access to resources

operations over resources

(once authenticated)

- Authorized
- NOT Authorized

3.4.8 Accounting

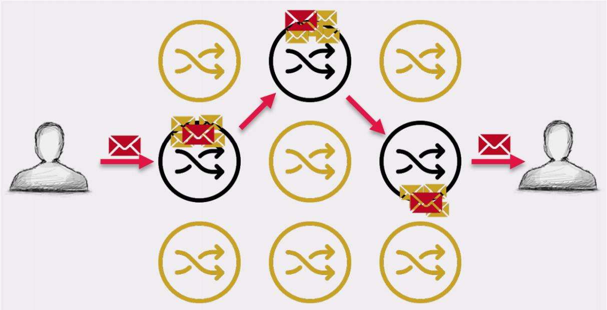


- Keeping track of information users and data
- Building and storing log data

3.5 MIX networks

- 1981 by David Chaum - "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms"
- anon.penet.fi
- Strong anonymity even against strong adversaries

3.5.1 Mixnets in a Nutshell



- Two key design decisions
  - Mix format
  - Mixing strategy
- Properties
  - Sender anonymity
  - Recipient anonymity
  - ...

3.5.2 The Anonymity Trilemma

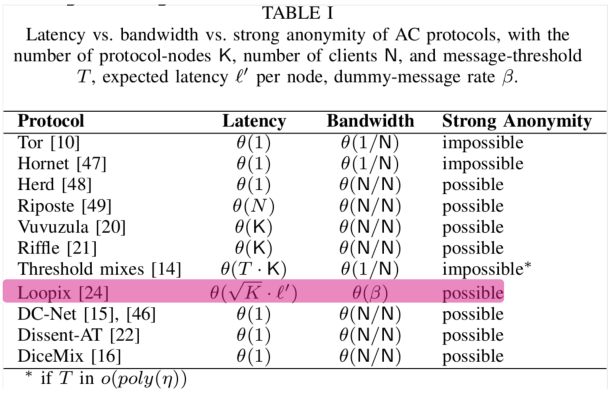


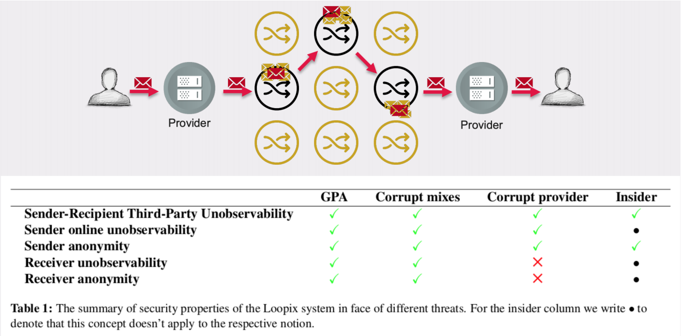
TABLE I

Latency vs. bandwidth vs. strong anonymity of AC protocols, with the number of protocol-nodes K, number of clients N, and message-threshold T, expected latency ℓ' per node, dummy-message rate β.

Protocol	Latency	Bandwidth	Strong Anonymity
Tor [10]	$\theta(1)$	$\theta(1/\mathsf{N})$	impossible
Hornet [47]	$\theta(1)$	$\theta(1/\mathsf{N})$	impossible
Herd [48]	$\theta(1)$	$\theta(\mathsf{N}/\mathsf{N})$	possible
Riposte [49]	$\theta(N)$	$\theta(\mathsf{N}/\mathsf{N})$	possible
Vuvuzula [20]	$\theta(\mathsf{K})$	$\theta(\mathsf{N}/\mathsf{N})$	possible
Riffle [21]	$\theta(\mathsf{K})$	$\theta(\mathsf{N}/\mathsf{N})$	possible
Threshold mixes [14]	$\theta(T \cdot \mathsf{K})$	$\theta(1/\mathsf{N})$	impossible*
Loopix [24]	$\theta(\sqrt{K} \cdot \ell')$	$\theta(\beta)$	possible
DC-Net [15], [46]	$\theta(1)$	$\theta(\mathsf{N}/\mathsf{N})$	possible
Dissent-AT [22]	$\theta(1)$	$\theta(\mathsf{N}/\mathsf{N})$	possible
DiceMix [16]	$\theta(1)$	$\theta(\mathsf{N}/\mathsf{N})$	possible

* if T in $o(poly(\eta))$

3.5.3 Loopix



	GPA	Corrupt mixes	Corrupt provider	Insider
Sender-Recipient Third-Party Unobservability	✓	✓	✓	✓
Sender online unobservability	✓	✓	✓	●
Sender anonymity	✓	✓	✓	✓
Receiver unobservability	✓	✓	✗	●
Receiver anonymity	✓	✓	✗	●

Table 1: The summary of security properties of the Loopix system in face of different threats. For the insider column we write ● to denote that this concept doesn't apply to the respective notion.

3.5.4 Wrapping Up

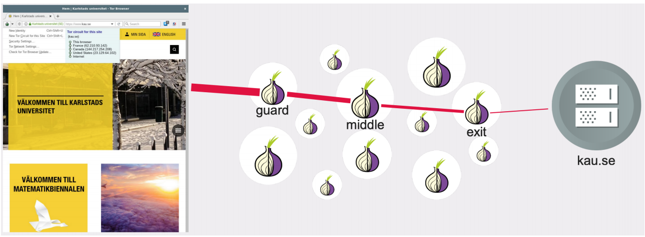
Panoramix
KU LEUVEN
greenhost.
grnet
SAP
UNIVERSITY OF TARTU
UCL
THE UNIVERSITY of EDINBURGH
HELLENIC REPUBLIC
National and Kapodistrian University of Athens
Funded by the European Union

- Strong anonymity, at the cost of latency and bandwidth
- All security from the mixing
  - Mix format and mixing strategy
- No wide deployments yet, but
  - Loopix and Sphinx
  - Panoramix and Katzenpost
- Applications beyond messaging: e-voting, surveys...

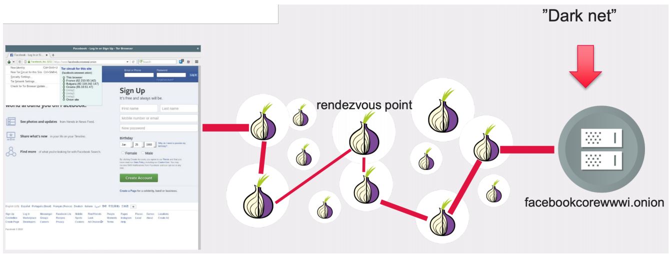
3.6 Tor in a Nutshell

- *The Tor project*, US non-profit 2006
  - Many projects: Tor Browser, Tor in a Nutshell Orbot, Tails, OONI...
  - Tor *network* of 6000 relays and 2000 bridges (> 48 Gbps)
  - *Low-latency anonymity network*
- Use cases
  - Anonymous browsing
  - Onion services
  - Single onion services
  - Censorship circumvention

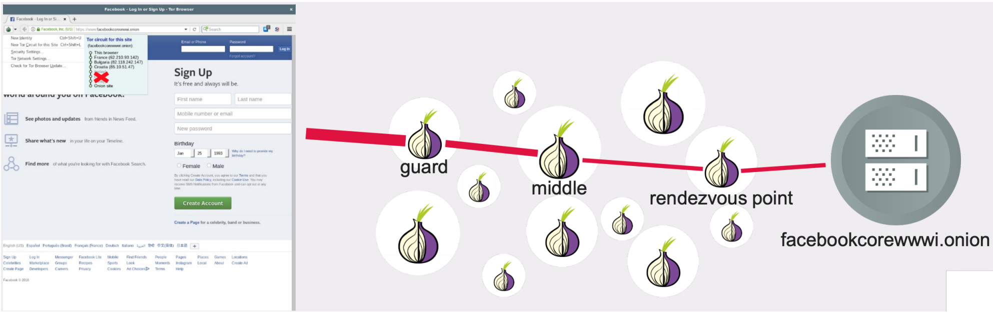
3.6.1 Anonymous Browsing


VÄLKOMMEN TILL KARLSTADS UNIVERSITET
VÄLKOMMEN TILL MATEMATIKBIENNALEN
guard
middle
exit
kau.se

3.6.2 Onion Services



3.6.3 Single Onion Services



Facebook - Log In or Sign Up - Tor Browser

Facebook - Log In or Si...

Facebook, Inc. (US) | https://www.facebookcorewwwi.onion

New Identity Ctrl+Shift+U
New Tor Circuit for this Site Ctrl+Shift+L
Security Settings...
Tor Network Settings...
Check for Tor Browser Update...

Tor circuit for this site
(facebookcorewwwi.onion):
This browser
France (62.210.93.142)
Bulgaria (82.118.242.147)
Croatia (85.10.51.47)
(relay)
(relay)
(relay)
Onion site

Email or Phone
Password
Log In
Forgot account?

Sign Up
It's free and always will be.
First name
Last name
Mobile number or email
New password
Birthday
Jan 25 1993
Why do I need to provide my birthday?
○ Female ○ Male
By clicking Create Account, you agree to our Terms and that you have read our Data Policy, including our Cookie Use. You may receive SMS Notifications from Facebook and can opt out at any time.
Create Account
Create a Page for a celebrity, band or business.

world around you on Facebook.
See photos and updates from friends in News Feed.
Share what's new in your life on your Timeline.
Find more of what you're looking for with Facebook Search.

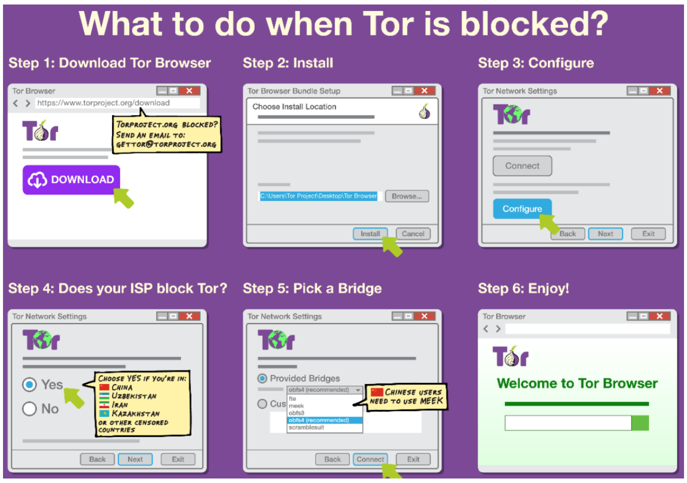
English (US) Español Português (Brasil) Français (France) Deutsch Italiano العربية हिन्दी 中文(简体) 日本語

Sign Up Log In Messenger Facebook Lite Mobile Find Friends People Pages Places Games Locations
Celebrities Marketplace Groups Recipes Sports Look Moments Instagram Local About Create Ad
Create Page Developers Careers Privacy Cookies Ad Choices Terms Help

Facebook © 2018

3.6.4 Censorship Circumvention

- Traffic exits at *exit relays*, bypasses national censors or regional restrictions
- → Censors block Tor
- Bridges are TOR entry points provided on a large scale



What to do when Tor is blocked?

Step 1: Download Tor Browser

Tor Browser
https://www.torproject.org/download
TORPROJECT.ORG BLOCKED? SEND AN EMAIL TO: GETTOR@TORPROJECT.ORG

Step 2: Install

Tor Browser Bundle Setup
Choose Install Location
C:\Users\Tor Project\Desktop\Tor Browser

Step 3: Configure

Tor Network Settings

Step 4: Does your ISP block Tor?

Tor Network Settings
● Yes
○ No
CHOOSE YES IF YOU'RE IN: CHINA, UZBEKISTAN, IRAN, KAZAKHSTAN OR OTHER CENSORED COUNTRIES

Step 5: Pick a Bridge

Tor Network Settings
● Provided Bridges
obfs4 (recommended)
fte
meek
obfs3
obfs4 (recommended)
scramblesuit
○ Cus
CHINESE USERS NEED TO USE MEEK

Step 6: Enjoy!

Tor Browser
Welcome to Tor Browser

3.6.5 Wrapping Up

- Tor is a *low latency network*, 6000 relays and 2000 bridges
- Anonymous browsing
  - Sender anonymity ("who is sending requests to a website?")
- Onion services & *single* onion services
  - Recipient anonymity ("who is receiving requests?")
  - Self authenticated, end-to-end encrypted, NAT punching, limit surface area
- Censorship circumvention

PROTECTING THE PRIVACY OF MILLIONS EVERY DAY
Tor: Powering Digital Resistance

3.7 Transparency Enhancing Tools (TETs)

3.7.1 Motivation: Transparency & Intervenability

- Legal privacy principles
  - *GDPR*:
    - General Art. 5 I (a) – lawfulness, fairness and transparency
    - Data subject rights to Transparency & Intervenability (GDPR – Chapter III)
  - *Swedish Data Patient Act*:
    - Rights to access health records and log information

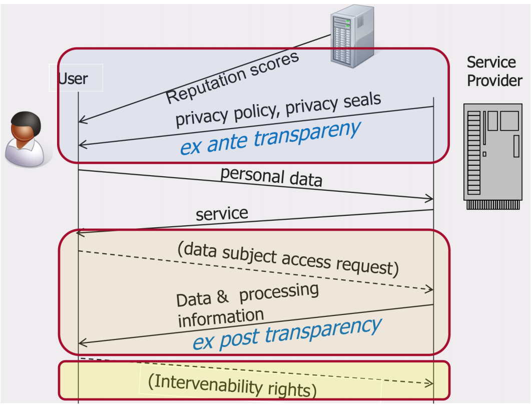
Examples

- **Log files in eHealth – privacy issues:**
  - Information about who (e.g., psychiatrist) accessed EHR is sensitive for patients
  - Monitoring of performance/quality of work of medical personnel
- **Business secrets in relation to profiling**
  - (cf. Recital 63 GDPR)

<u>Requirements</u>

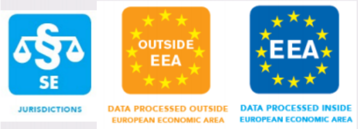
- Privacy-preserving

- Considering Tradeoffs with rights of others

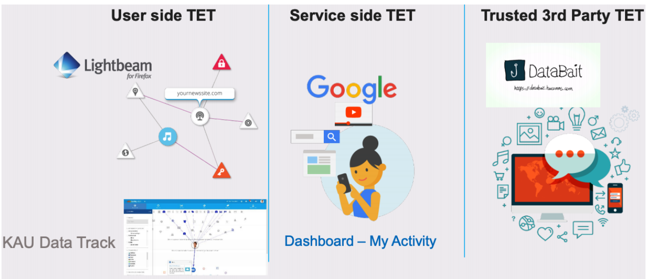


3.7.2 Ex-ante TETs - Examples

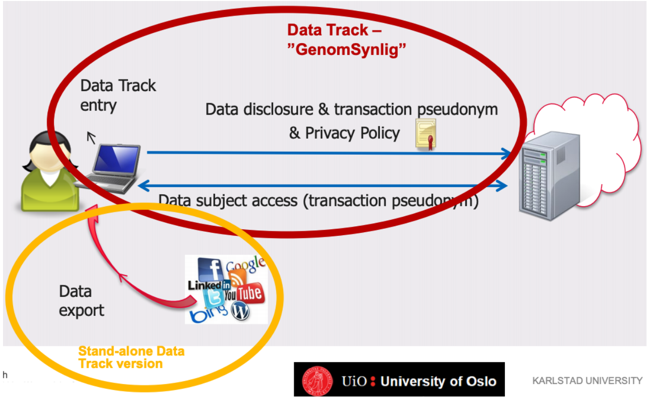
- Privacy Policy Languages: e.g., P3P, PPL, A-PPL
- Multi-Layered Structured Policies (Art. 29 WP), complemented by Policy Icons, Examples:
  Examples of suggested Cloud-specific policy icons (A4Cloud):


SE
JURISDICTIONS
OUTSIDE EEA
DATA PROCESSED OUTSIDE EUROPEAN ECONOMIC AREA
EEA
DATA PROCESSED INSIDE EUROPEAN ECONOMIC AREA

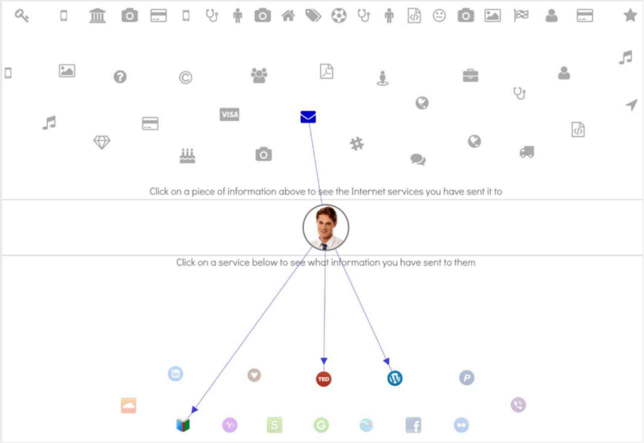
3.7.3 Ex post TETs - Examples



3.7.4 User controlled ex post TET: Data Track


Data Track – ”GenomSynlig”
Data Track entry
Data disclosure & transaction pseudonym
& Privacy Policy
Data subject access (transaction pseudonym)
Data export
Stand-alone Data Track version
UiO : University of Oslo
KARLSTAD UNIVERSITY

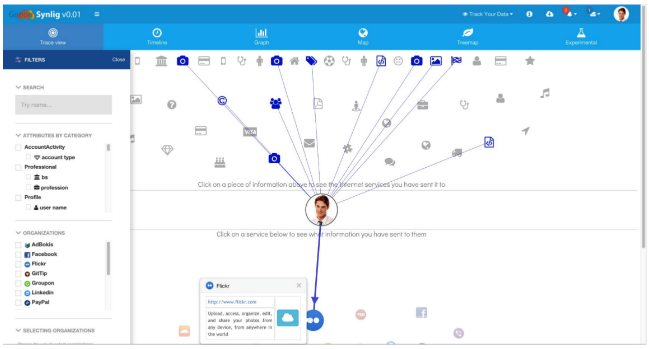
Data Track – Trace View: Viewing attributes in common



Click on a piece of information above to see the Internet services you have sent it to

Click on a service below to see what information you have sent to them

Trace View – What does a service provider know about me?



Try name...

Click on a piece of information above to see the Internet services you have sent it to

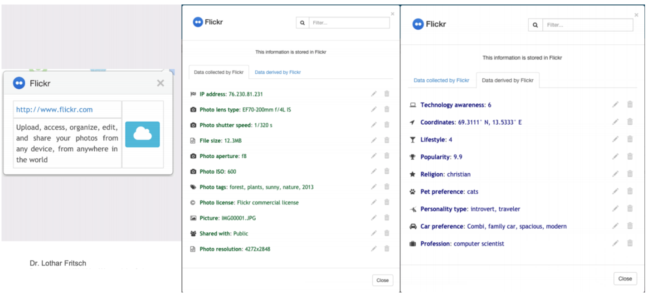
Click on a service below to see what information you have sent to them

Flickr

http://www.flickr.com

Upload, access, organize, edit, and share your photos from any device, from anywhere in the world

Online Access View & Intervenability functions



Flickr

http://www.flickr.com

Upload, access, organize, edit, and share your photos from any device, from anywhere in the world

Dr. Lothar Fritsch

Flickr

Filter...

This information is stored in Flickr

IP address: 76.230.81.231
Photo lens type: EF70-200mm f/4L IS
Photo shutter speed: 1/320 s
File size: 12.3MB
Photo aperture: f8
Photo ISO: 600
Photo tags: forest, plants, sunny, nature, 2013
Photo license: Flickr commercial license
Picture: IMG00001.JPG
Shared with: Public
Photo resolution: 4272x2848

Flickr

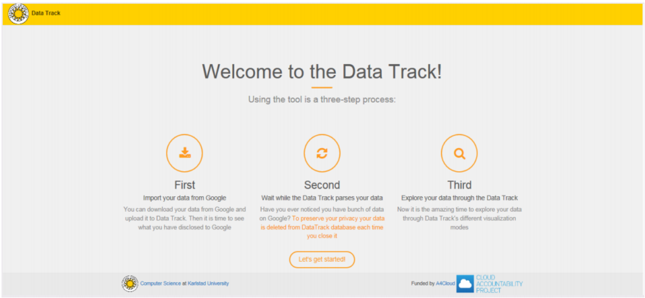
Filter...

This information is stored in Flickr

Technology awareness: 6
Coordinates: 69.3111° N, 13.5333° E
Lifestyle: 4
Popularity: 9.9
Religion: christian
Pet preference: cats
Personality type: introvert, traveler
Car preference: Combi, family car, spacious, modern
Profession: computer scientist

Data Track visualising Data Exports

Open-source standalone Data Track
(https://github.com/pylls/datatrack)



Welcome to the Data Track!

Using the tool is a three-step process:

First

Import your data from Google

You can download your data from Google and upload it to Data Track. Then it is time to see what you have disclosed to Google

Second

Wait while the Data Track parses your data

Have you ever noticed you have bunch of data on Google? To preserve your privacy your data is deleted from DataTrack database each time you close it

Third

Explore your data through the Data Track

Now it is the amazing time to explore your data through Data Track's different visualization modes

Let's get started!
Computer Science at Karlstad University
Funded by A4Cloud
CLOUD ACCOUNTABILITY PROJECT

3.8 Summary

Privay protection consists of:

- Protection of communication content
- Protection of communication relationship
- Protection of identities
- Concealment of own activity against others' observation
- Unlinkablility between different actions
- Transparency of collection, processing and storage
- Intervenability and rectification opportunities

4 Lecture 4: Privacy by Design, Privacy protection goals

4.1 Content

- Privacy vs. Data protection
- Privacy by Design principles
- Privacy goals
- Privacy paradigms

4.1.1 Privacy $\neq$ Data Protection

- Privacy is fuzzy, contextual, social construct, depends...
- Data protection, by necessity, has to be more discrete.
- Proportionality of data processing is a key consideration.

→ Data protection necessary but not sufficient for privacy

4.2 Ann Cavoukian's Seven Privacy by Design Principles

- Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.
- Privacy by Design extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure.

Overview

- Seven principles, by Ann Cavoukian, Information and Privacy Commissioner of Ontario/Canada
- End of 1990's $\sim$ beginning of 2000's
- Data protection centric (control, see paradigms later in the course)

4.3 Seven Privacy by Design Principles

1. **Proactive** not Reactive; **Preventative** not Remedial

   The Privacy by Design approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred - it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.

2. Privacy as the **Default**

   We can all be certain of one thing - the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy - it is built into the system, by default.

3. Privacy **Embedded** into Design

   Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. **Full** Functionality – Positive-Sum, **not Zero-Sum**

   Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretence of false dichotomies, such as privacy vs. security, demonstrating that it is possible, and far more desirable, to have both.

5. End-to-End Security – Full **Lifecycle** Protection

   Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved - strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end.

6. Visibility and Transparency – Keep it **Open**

   The Privacy by Design approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred - it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.

7. Respect for User Privacy - Keep it **User-Centric**

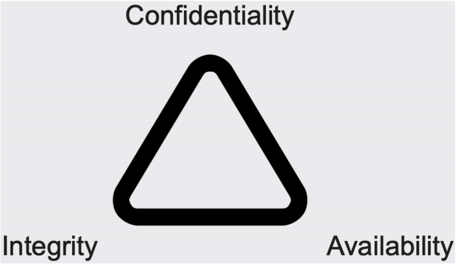
   Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric!

So what shall a software developer do with PbD?

- PbD principles do not provide any hands-on instructions for software engineers or developers.
- Ask yourself: "How shall I implement principle X?" X € {1,..,7}

4.4 Privacy goals

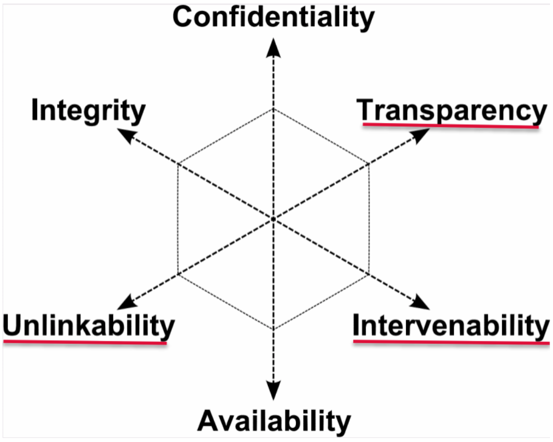
4.4.1 Information Security: The CIA triad



4.4.2 Complementing CIA with privacy

- Add privacy to the security triad
  - CIA already considered in procedures, processes etc.
  - → privacy protection goals help with including privacy
- Three important privacy goals
- Originate in German data protection community

4.5 Privacy Protection Goals



Protection goals as seen by Standard Data Protection Model

- The Standard Data Protection Model v1.0, 2016

  $https://www.datenschutzzentrum.de/sdm/$

  $https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V1.0.pdf$
- The data protection supervisory authorities of the German states and the federal government use the **Standard Data Protection Model** (SDM) to describe a model to systematically verify compliance with statutory requirements relating to the handling of personal data and their appropriate **implementation**.

4.5.1 Confidentiality

Typical measures to guarantee confidentiality are:

- Definition of rights and role access control based on need-to-know as part of identity management by the controller,
- Implementation of a secure authentication process,
- Limitation of authorized personnel to those who are verifiably responsible (locally, professionally), qualified, reliable (if necessary with security clearance) and formally approved, and with whom no conflict of interests may arise in the exercise of their duties,
- Specification and control of the use of approved resources, in particular communication channels,
- Specified environments (buildings, rooms) equipped for the procedure,
- Specification and control of organisational procedures, internal regulations and contractual obligations (obligation to data secrecy, confidentiality agreements, etc.),
- Encryption of stored or transferred data as well as establishing processes for the management and protection of the cryptographic information (cryptographic concept),
- Protection against external influences (espionage, hacking).

4.5.2 Transparency

Typical measures to guarantee transparency are:

- Documentation of procedures, including the business processes, data stocks, data flows and the IT systems used, operating procedures, description of procedure, interaction with other procedures,
- Documentation of testing, approval and, where appropriate, prior checking of new or modified procedures,
- Documentation of contracts with internal employees; contracts with external service providers and 3rd parties, from which data are collected or transferred to; business distribution plans, internal responsibility assignments,
- Documentation of consents and objections,
- Logging of access and modifications,
- Verification of data sources (authenticity),
- Version control,
- Documentation of the processing procedures by means of protocols on the basis of a logging and evaluation concept,
- Consideration of the data subject's rights in the logging and evaluation concept.

4.5.3 Intervenability

Typical measures to guarantee intervenability are:

- Differentiated options for consent, withdrawal and objection,
- Creating necessary data fields, e.g. for blocking indicators, notifications, consents, objections, right of reply,
- Documented handling of malfunctions, problem-solving methods and changes to the procedure as well as to the protection measures of IT security and data protection,
- Disabling options for individual functionalities without affecting the whole system,
- Implementation of standardised query and dialogue interfaces for the persons concerned to assert and/or enforce claims,
- Traceability of the activities of the controller for granting the data subject's rights,
- Establishing a Single Point of Contact (SPoC) for data subjects,
- Operational possibilities to compile, consistently correct, block and erase all data stored with regard to any one person..

4.5.4 Availability

Typical measures to guarantee availability are:

- Preparation of data backups, process states, configurations, data structures, transaction histories etc., according to a tested concept,
- Protection against external influences (malware, sabotage, force majeure),
- Documentation of data syntax,
- Redundancy of hard- and software as well as infrastructure,
- Implementation of repair strategies and alternative processes,
- Rules of substitution for absent employees.

4.5.5 Unlinkability

Typical measures to guarantee unlinkability are:

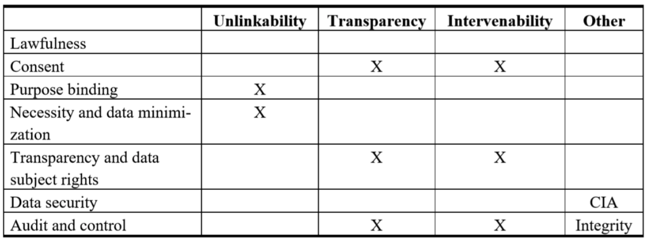
- Restriction of processing, utilization and transfer rights,
- In terms of programming, omitting or closing of interfaces in procedures and components of procedures,
- Regulative provisions to prohibit backdoors as well as establishing quality assurance revisions for compliance in software development,
- Separation in organizational / departmental boundaries,
- Separation by means of role concepts with differentiated access rights on the basis of an identity management by the responsible authority and a secure authentication method,
- Approval of user-controlled identity management by the data processor,
- Using purpose specific pseudonyms, anonymity services, anonymous credentials, processing of pseudonymous or anonymous data,
- Regulated procedures for purpose amendments.

4.5.6 Integrity

Typical measures to guarantee integrity or to assess a breach of integrity are:

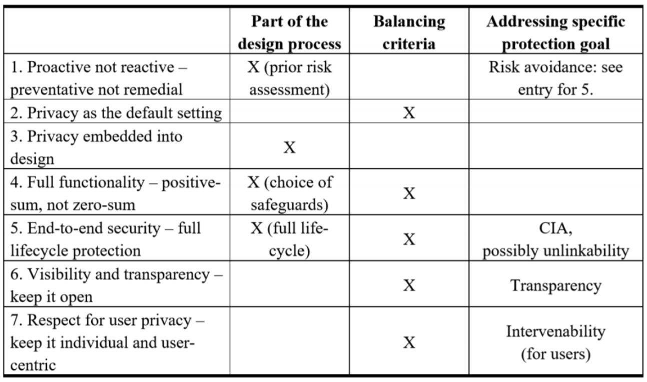
- Restriction of writing and modification permissions,
- Use of checksums, electronic seals and signatures in data processing in accordance with a cryptographic concept,
- Documented assignment of rights and roles,
- Processes for maintaining the timeliness of data,
- Specification of the nominal process behavior and regular testing for the determination and documentation of functionality, of risks as well as safety gaps and the side effects of processes,
- Specification of the nominal behavior of workflow or processes and regular testing of the detectability respective determination of the current state of processes.

4.5.7 Goals vs. Principles



	Unlinkability	Transparency	Intervenability	Other
Lawfulness				
Consent		X	X	
Purpose binding	X			
Necessity and data minimization	X			
Transparency and data subject rights		X	X	
Data security				CIA
Audit and control		X	X	Integrity

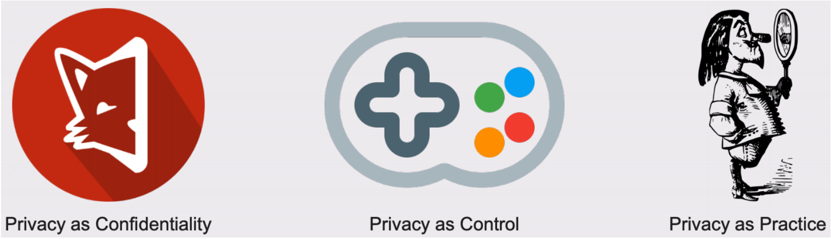
4.5.8 Privacy by Design vs. Principles



	Part of the design process	Balancing criteria	Addressing specific protection goal
1. Proactive not reactive – preventative not remedial	X (prior risk assessment)		Risk avoidance: see entry for 5.
2. Privacy as the default setting		X	
3. Privacy embedded into design	X		
4. Full functionality – positive-sum, not zero-sum	X (choice of safeguards)	X	
5. End-to-end security – full lifecycle protection	X (full life-cycle)	X	CIA, possibly unlinkability
6. Visibility and transparency – keep it open		X	Transparency
7. Respect for user privacy – keep it individual and user-centric		X	Intervenability (for users)

4.6 Privacy Paradigms

Three Privacy (Research) Paradigms



4.6.1 Privacy as Confidentiality

- Data disclosed → privacy lost
- Data minimization
- Centralized → bad
- Cryptography community
- Open source, reproducibility

4.6.2 Privacy as Control

- Ability to exercise control over personal data → privacy
- May be in your interest to disclose personal data (e.g., healthcare)
- Data protection
  - Purpose
  - Intervenability
  - Transparency
  - Accountability

4.6.3 Privacy as Practice

- Freedom to understand and control privacy decisions
- Industry: "do not scare users"
  - Over time, get people to share more and more about themselves, but not perceive it as invasive
- Like a mirror
  - Understand how you are perceived
  - Control how you are perceived
  - Feedback and nudges

4.6.4 Designing for "Privacy"?

- Neither pradigm is wrong, neither prioritized
- Industry likes privacy as practice, self-regulation
  - For the wrong reasons? (more data)
  - But does also good?
- GDPR
  - Privacy as control
  - Data minimisation important principle
  - High fines → personal data is a risk → push for privacy as confidentiality?

4.7 10 common privacy design mistakes

- Author works with a data protection agency in Germany.
- Article summarizes frequently seen mistakes in privacy design.

Hansen, M. (2011, September). Top 10 mistakes in system design from a privacy perspective and privacy protection goals. In IFIP PrimeLife International Summer School on Privacy and Identity Management for Life (pp. 14-31). Springer, Berlin, Heidelberg.

4.7.1 Mistake 1: Storage as Default

- No reasoning about storage justification, period and access control.
- Violates data minimization, purpose binding, right to be forgotten.

4.7.2 Mistake 2: Linkability as Default

- No unidentified use of prodct or service possible.
- Linking between different transactions.
- Profiling risk.
- May violate data minimization, purpose-binding.

4.7.3 Mistake 3: Real Name as Default

- Real names, e-mail addresses, phone numbers as part of profile / identity or data set.
- Without pseudonyms there is no unlinkability from the private life.
- However, not many system designers consider pseudonyms, and even if the state in their privacy policy that pseudonyms are accepted, this is not always reflected in their forms and database schemas that contain a mandatory first name and last name.

4.7.4 Mistake 4: Function Creep as Feature

- "Function creep" means a widening of the data processing beyond the original purpose or context.
- Violates the principle of purpose binding and can pose risks to privacy that have to be considered when assessing the system.
- Code re-use practices and evolution of IT systems often cause function creep.
- Personal data or processing algorithms "creep" over to new purposes.

4.7.5 Mistake 5: Fuzzy or Incomplete Information as Default

- Vague, generalized privacy policy vocabulary avoids precision.
- Ill-defined purposes and flexible specification of system related to dynamic business model quite frequent.
- Too broad specification for developers opens for interpretation risks.

4.7.6 Mistake 6: "Location Does Not Matter"

- Location of processing data matters in law.
- Privacy law valid in jurisdictions – different jurisdictions, different rules.
- Export of personal data over national borders is regulated.
- Technology is globalized (cloud, VM, SAAS, location of actual data lines and radio links), developers know little about deployment location.

Issues:

- U.S: Homeland Security legislation allows government data seizure.
- Social media corporations cooperate with Chinese authorities.
- Swedish Intelligence law permits interception of all cross-border data traffic.

4.7.7 Mistake 7: No Lifecycle Assessment

- Many problems occur because the system design did not consider the full lifecycle of the data, the organization or the system itself.
- Data created without a removal plan.
- No data lifecycle management implemented – database just grows.
- Often poor control over data deletion at suppliers when changing e.g. a cloud provider

4.7.8 Mistake 8: Changing Assumptions or Surplus Functionality

- A later change in purpose or specification can endanger privacy of data already processed on a system.
- Even if we assume that a privacy-compliant service with exemplary data minimization and transparency has been developed, adding additional functionality may water down or even contradict the intended privacy guarantees.
- In particular, a surplus payment method, a business model basing on profiling and advertising, or obligations from the police or homeland security could render all privacy efforts useless.

4.7.9 Mistake 9: No Intervenability Foreseen

- System is designed to process data to solve a specific task.
- Intervenability adds severe complexity – often not part of specification.
- Developers often try to avoid full intervenability through delegation to legal department. This leads to expensive and time-consuming manual database extraction efforts for each data subject inquiry.

4.7.10 Mistake 10: Consent Not Providing a Valid Legal Ground

- Data subject consent legally not sufficient – but developers presume it is.
- "Forced consent" where there is no other choice.
- Information about processing insufficient (e.g. poor, outdated or incomplete privacy policy)
- Unproportionality of collection or processing – even with consent.

4.8 Privacy impact analysis (PIA)

- Security measures and privacy protection shall correspond to the risks of a data breach and the impact it will cause on data subjects.
- PIA or DPIA (Data protection analysis) are an approach to map risks and impact that helps understand the stakes.

4.8.1 Perceiving PIAs as Mandatory

- PIAs are not mandatory, DPIAs only in particular cases
- May lead to "PIA fatigue"

4.8.2 Not Adapting Questions

- Same questionnaire for assessing data processing
- Different needs for different activities
- Should first perform a light- weight PIA to determine if full PIA is necessary

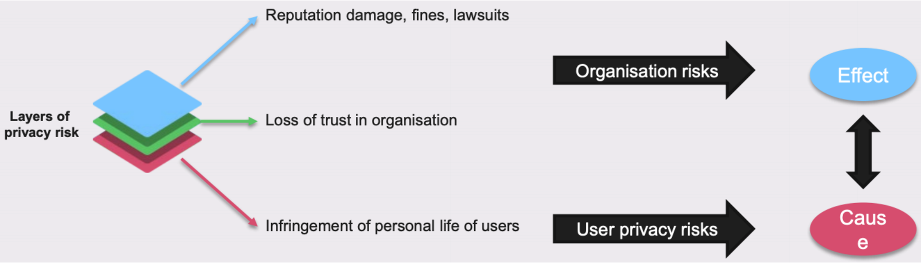
4.8.3 Focus on the Wrong Stakeholder

- Organisation-centric, to avoid fines
- Should be user-centric, and consult users as part of PIA

4.8.4 PIA as a Task

- Treating PIA as a one-time task early in development
- Revised years after first creation
- PIA is a process, not a task

4.8.5 Mixing Cause and Effect


Layers of privacy risk
Reputation damage, fines, lawsuits
Loss of trust in organisation
Infringement of personal life of users
Organisation risks
User privacy risks
Effect
Caus
e

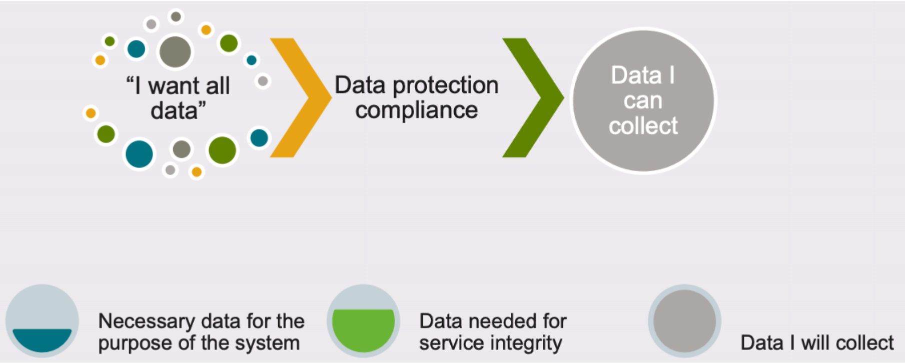
4.8.6 Conclusions

- Five common mistakes
  1. Perceiving PIAs as mandatory
  2. Not adapting questions
  3. Focus on the wrong stakeholder
  4. PIA as a task
  5. Mixing cause and effect
- Being organisation-centric instead of user-centric
  - PIAs (at best) → data protection compliance
  - → no privacy-friendly systems
- Focus on avoiding risks, not only mitigating

4.8.7 Designing for Privacy

- Privacy is multifaceted
  - An essential human right, data protection closely related
  - Paradigms as confidentiality, control, practice
  - CIA+Unlinkability+Transparency+Intervenability
- DPIAs/PIAs are essential to design for privacy
  - A process, understanding privacy risks
  - Added value for organization: incident response, risks related to GDPR
- Data protection by design and by default
  - Reasonable measures, protect rights, full life-cycle
  - Strong protections by default
  - Depends on how the GDPR is enforced and interpreted

4.9 Change of Mindset


"I want all data"
Data protection compliance
Data I can collect
Necessary data for the purpose of the system
Data needed for service integrity
Data I will collect

4.10 Privacy Engineering

- Newly formed field of research and practice
- From tradecraft and know-how to engineering
- We don't really have good and solid methods, but we have starting points that show promise
  - PIAs we already covered
  - Chapters 4 & 5 on Privacy Management touch on high-level analysis methods, like LINDDUN
  - Chapter 6 on Privacy Patterns for Software Design covers software engineering perspective

5 Lecture 5: Privacy Impact Assessment, Privacy Risk Assessment

Overview

- Privacy Impact Assessment (PIA)
  - What is it? How to use it?
- Privacy Risk Assessment
  - What is IT risk management?
  - What is qualitative risk assessment?
  - What is privacy risk assessment?

5.1 Privacy Impact Assessment: Definition

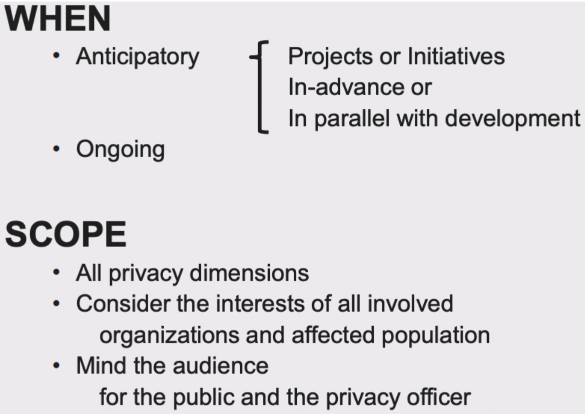
A Privacy Impact Assessment (PIA) is a systematic process for identifying and addressing privacy issues in an information system that considers the future consequences for privacy of a current or proposed action.

However, in some jurisdictions the deliverable of the PIA process is a document, such as a PIA report, which is a predictive exercise that looks to prevent or minimize the adverse effects on privacy.

5.1.1 PIA Objective

- Understand privacy-related concerns
  - Produce better policies and systems
- **WHY**
  - Mitigate risks to business (reduce costs), users (reduce burden and intransparency), and society (by strengthening the rule of law).
  - Comply with legal and regulatory obligations
  - Meet expectations of individuals
- **FOR**
  - Services
  - Systems
  - Products
  - Policies

5.1.2 PIA Timing and Scope



WHEN

- Anticipatory
- Ongoing

Projects or Initiatives
In-advance or
In parallel with development

SCOPE

- All privacy dimensions
- Consider the interests of all involved organizations and affected population
- Mind the audience for the public and the privacy officer

5.1.3 The Core PIA elements

1. An on-going process
2. Scalability
3. All privacy types
4. Privacy vs. data protection
5. Beyond PIA
6. Terminology
7. Accountability
8. Transparency
9. Stakeholders' involvement
10. Publication of the PIA report
11. Central public registry
12. Sensitive information
13. Risks management and legal compliance check
14. Audit and review

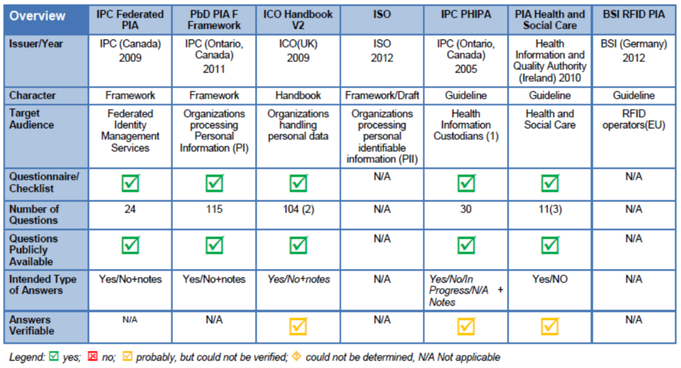
5.1.4 The PIA process

1. Early start
2. Project description
3. General description of the project
4. Information flows and other privacy implications
5. Stakeholders' consultation
6. Identification
7. Information
8. Consultation
9. Consideration
10. Risks management
11. Risks assessment
12. Risks mitigation
13. Legal compliance check
14. Recommendations and report
15. Decision and implementation of recommendations
16. Audit and review

5.1.5 Privacy risk & impact

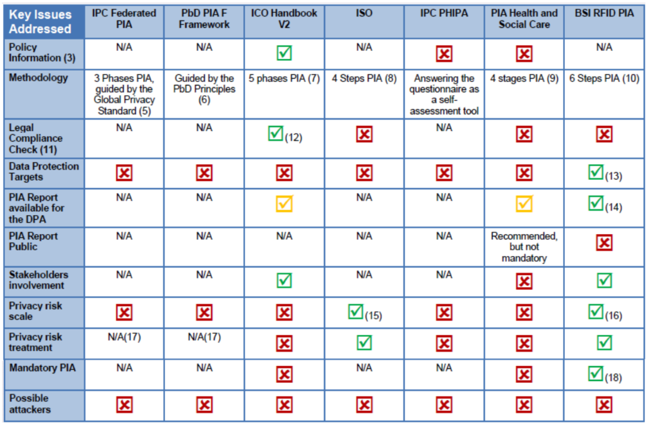
- The assessor should identify, assess and mitigate all possible risks and other negative privacy impacts. Residual risks should be justified.
- Any risk management is only as good as the methodology underlying it. This means if the methodology is flawed, then so is the assessment.
- The risk assessment should take into account the impacts on both the individual and on society.
- A PIA process requires a relative quantification of these risks. The Assessor should consider the likelihood and consequences of privacy risks occurring. Finally, the risk assessment requires evaluating the applicable risks. Thus the assessor should consider: (1) the significance of a risk and the likelihood of its occurrence, and (2) the magnitude of the impact should the risk occur. The resulting risk level can then be classified as low, medium or high.
- Based on risk assessment: Define controls for privacy risk!
- Preventive controls (prevent violation) or detective controls (detect violation)
- Technical controls: go into project (e.g. security and PET mechanisms, anonymity, data minimization).
- Non-technical controls get implemented in processes, procedures, policies and operations.

5.1.6 PIA Standards Overview



Overview	IPC Federated PIA	PbD PIA F Framework	ICO Handbook V2	ISO	IPC PHIPA	PIA Health and Social Care	BSI RFID PIA
Issuer/Year	IPC (Canada) 2009	IPC (Ontario, Canada) 2011	ICO(UK) 2009	ISO 2012	IPC (Ontario, Canada) 2005	Health Information and Quality Authority (Ireland) 2010	BSI (Germany) 2012
Character	Framework	Framework	Handbook	Framework/Draft	Guideline	Guideline	Guideline
Target Audience	Federated Identity Management Services	Organizations processing Personal Information (PI)	Organizations handling personal data	Organizations processing personal identifiable information (PII)	Health Information Custodians (1)	Health and Social Care	RFID operators(EU)
Questionnaire/ Checklist	☑	☑	☑	N/A	☑	☑	N/A
Number of Questions	24	115	104 (2)	N/A	30	11(3)	N/A
Questions Publicly Available	☑	☑	☑	N/A	☑	☑	N/A
Intended Type of Answers	Yes/No+notes	Yes/No+notes	*Yes/No+notes*	N/A	*Yes/No/In Progress/N/A + Notes*	Yes/NO	N/A
Answers Verifiable	N/A	N/A	✓	N/A	✓	✓	N/A

Legend: ☑ yes; ☒ no; ✓ probably, but could not be verified; ◇ could not be determined, N/A Not applicable



Key Issues Addressed	IPC Federated PIA	PbD PIA F Framework	ICO Handbook V2	ISO	IPC PHIPA	PIA Health and Social Care	BSI RFID PIA
Policy Information (3)	N/A	N/A	☑	N/A	☒	☒	N/A
Methodology	3 Phases PIA, guided by the Global Privacy Standard (5)	Guided by the PbD Principles (6)	5 phases PIA (7)	4 Steps PIA (8)	Answering the questionnaire as a self-assessment tool	4 stages PIA (9)	6 Steps PIA (10)
Legal Compliance Check (11)	N/A	N/A	☑(12)	☒	N/A	☒	☒
Data Protection Targets	☒	☒	☒	☒	☒	☒	☑(13)
PIA Report available for the DPA	N/A	N/A	✓	N/A	N/A	✓	☑(14)
PIA Report Public	N/A	N/A	N/A	N/A	N/A	Recommended, but not mandatory	☒
Stakeholders involvement	N/A	N/A	☑	N/A	N/A	☒	☑
Privacy risk scale	☒	☒	☒	☑(15)	☒	☒	☑(16)
Privacy risk treatment	N/A(17)	N/A(17)	☒	☑	☒	☒	☑
Mandatory PIA	N/A	N/A	☒	N/A	N/A	☒	☑(18)
Possible attackers	☒	☒	☒	☒	☒	☒	☒

5.2 Summary

5.2.1 PIA privacy target

- privacy of **personal information;**
- privacy of the **person;**
- privacy of **personal behavior;** and
- privacy of **personal communications**

5.2.2 PIA results

The outcome of PIA is expected to:

- identify of the project's privacy impacts;
- assess those impacts from the perspectives of all stakeholders;
- understand the acceptability of the project and its features by the organizations and people who will be affected by it;
- identify and assess of less privacy-invasive alternatives;
- show how negative impacts on privacy can be avoided;
- lessen negative impacts on privacy;
- clarify, where negative impacts on privacy are unavoidable, the business need that justifies them;
- document and publish of the outcomes.

5.2.3 Content of PIA report

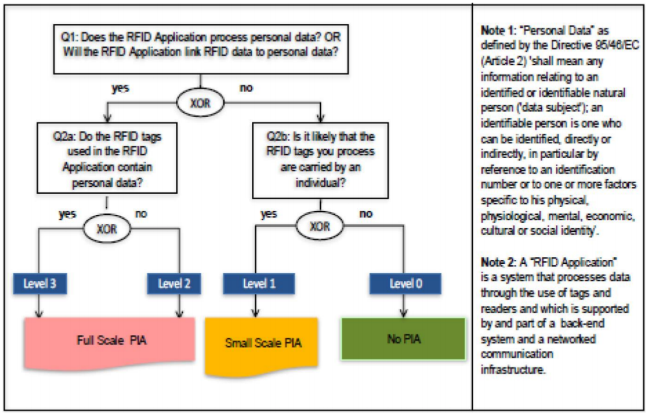
A PIA report contains

- a description of the project;
- an analysis of the privacy issues arising from it;
- the business case justifying privacy intrusion and its implications;
- a discussion of alternatives considered and the rationale for the decisions made;
- a description of the privacy design features adopted to reduce and avoid privacy intrusion and their implications of these design features;
- an analysis of the public acceptability of the scheme and its applications.

5.2.4 Content of PIA report

- a PIA is anticipatory in nature, conducted in advance of or in parallel with the development of an initiative, rather than retrospectively;
- a PIA has broad scope in relation to the dimensions of privacy, enabling consideration of privacy of the person, privacy of personal behaviour and privacy of personal communications, as well as privacy of personal data;
- a PIA has broad scope in relation to the perspectives reflected in the process, taking into account the interests not only of the sponsoring organization, and of the sponsor's strategic partners, but also of the population segments affected by it, at least through representatives and advocates;
- a PIA is performed on a project or initiative;
- a PIA has broad scope in relation to the expectations against which privacy impacts are compared, including people's aspirations and needs, and public policy considerations, as well as legal requirements;
- a PIA is oriented towards the surfacing both of problems and of solutions to them;
- a PIA emphasises the assessment process including information exchange, organisational learning, and design;
- a PIA requires intellectual engagement from executives and senior managers.

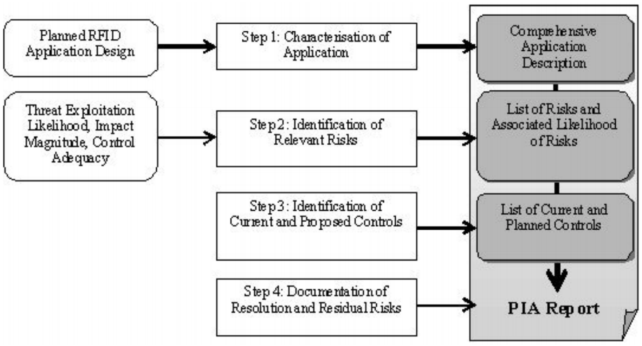
[EU-RFID]: Small scale or full scale PIA?


Q1: Does the RFID Application process personal data? OR Will the RFID Application link RFID data to personal data?
yes
XOR
no
Q2a: Do the RFID tags used in the RFID Application contain personal data?
Q2b: Is it likely that the RFID tags you process are carried by an individual?
yes
XOR
no
yes
XOR
no
Level 3
Level 2
Level 1
Level 0
Full Scale PIA
Small Scale PIA
No PIA

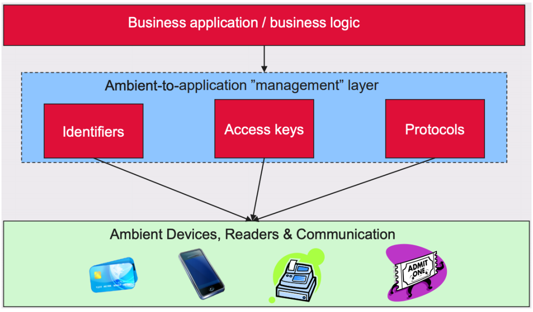
Note 1: "Personal Data" as defined by the Directive 95/46/EC (Article 2) 'shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.

Note 2: A "RFID Application" is a system that processes data through the use of tags and readers and which is supported by and part of a back-end system and a networked communication infrastructure.

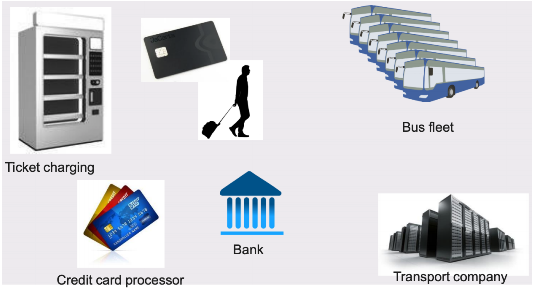
[EU-RFID]: PIA process


Planned RFID Application Design
Threat Exploitation Likelihood, Impact Magnitude, Control Adequacy
Step 1: Characterisation of Application
Step 2: Identification of Relevant Risks
Step 3: Identification of Current and Proposed Controls
Step 4: Documentation of Resolution and Residual Risks
Comprehensive Application Description
List of Risks and Associated Likelihood of Risks
List of Current and Planned Controls
PIA Report

PIA Application Example: [EU-RFID] (2011)


Business application / business logic
Ambient-to-application "management" layer
Identifiers
Access keys
Protocols
Ambient Devices, Readers & Communication
ADMIT ONE

Case study: RFID bus ticket



PIA Future

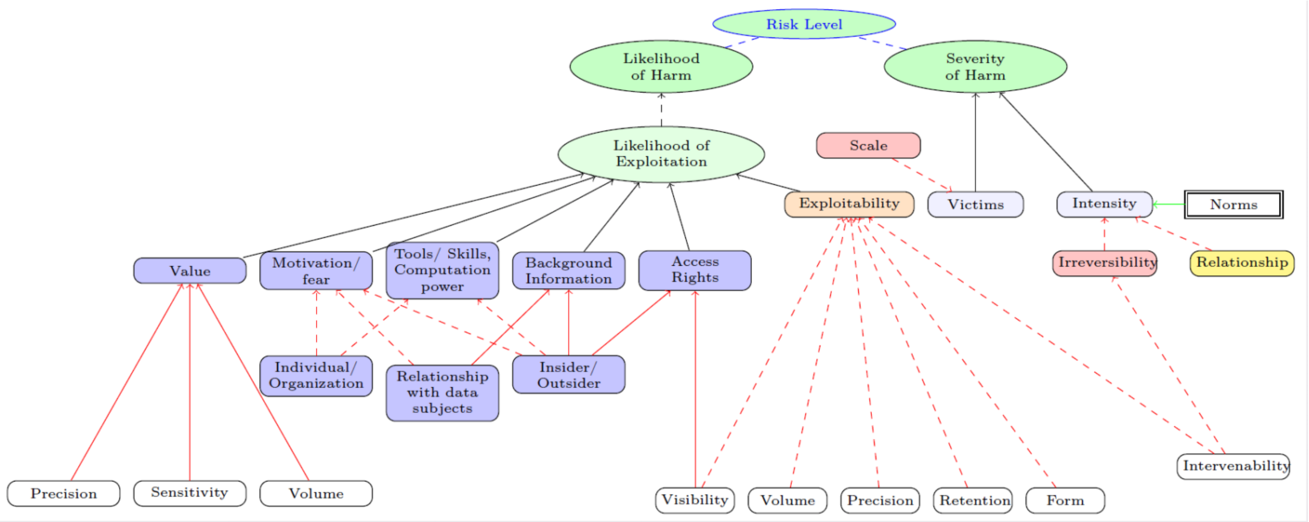
- In the PIAF project, a thorough analysis of PIA needs and its future develoment path has been made [PIAF-D3].
- In particular, PIAF concludes that: A PIA should be regarded and carried out as a process and not only as a single task of completion of a report. A PIA process starts early and continues throughout the life cycle of the project.

5.3 Privacy Risk Assessment

In this part of the lecture, we will look at:

- A short introduction / recapitulation of risk management
- An introduction of risk assessment
- Privacy risk assessment and privacy risk
- Difficulties and issues with privacy risk assessment

5.3.1 PRIAM privacy risk methodology



5.3.2 PRIAM privacy harms (impact)

Definition: A privacy harm is the negative impact on a data subject, or a group of data subjects, or the society as a whole, from the standpoint of physical, mental, or financial well-being or reputation, dignity, freedom, acceptance in society, self-actualization, domestic life, freedom of expression, or any fundamental right, resulting from one or more feared events.

5.3.3 PRIAM categories of privacy harm

1. Physical harms
2. Economic or financial harms
3. Mental or psychological harms
4. Harms to dignity or reputation
5. Societal or architectural harms

Each harm has two attributes:

1. Victim
2. Intensity

5.4 Definitions

Definitions (from ISO 13335-1 and ISO 27001)

- **Risk Acceptance**: decision to accept a risk
- **Risk Analysis**: systematic use of information to identify sources and to estimate the risk
- **Risk Assessment**: overall process of risk analysis and risk evaluation
- **Risk Evaluation**: process of comparing the estimated risk against given risk criteria to determine the significance of the risk
- **Risk Management**: coordinated activities to direct and control an organization with regard to risk
- **Risk Treatment**: process of selection and implementation of measures to modify risk
- **Statement of Applicability**: documented statement describing the control objectives and controls that are relevant and applicable to the organization's ISMS

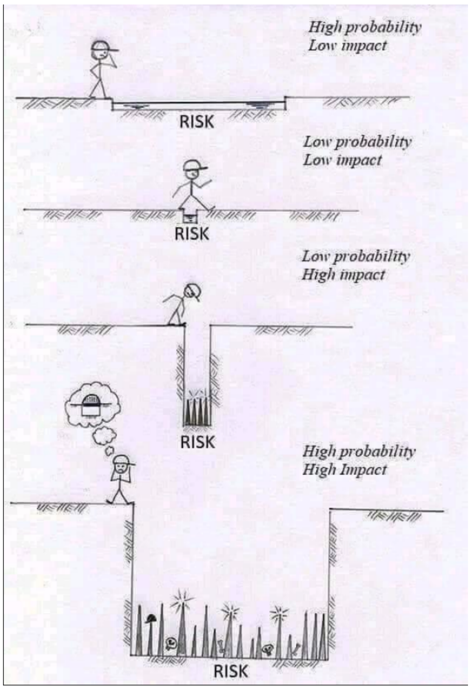
5.4.1 What is risk assessment?

Risk Assessment: a systematic study of assets, threats, vulnerabilities and impacts (consequences) to assess the probability and consequences of risk
Risk Management is a formalized process; (planned, input data recorded, analysis and results should be recorded)

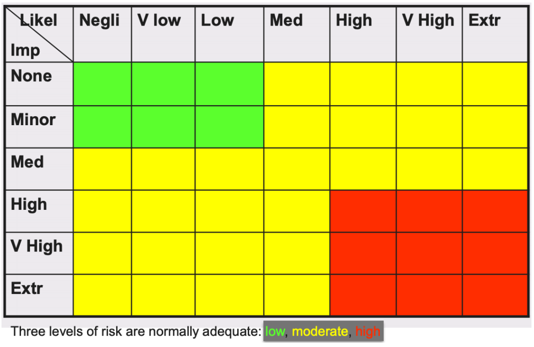
5.4.2 Qualitative Risk Assessment

- Uses likelihood and impact of events on assets
- Based on historic data for both likelihood and impact
- In new settings often guesswork

Loss(A) = impact(T(A))*likelihood(T(A)) where T(A) is threat T effective on asset A.



5.4.3 Risk assessment form



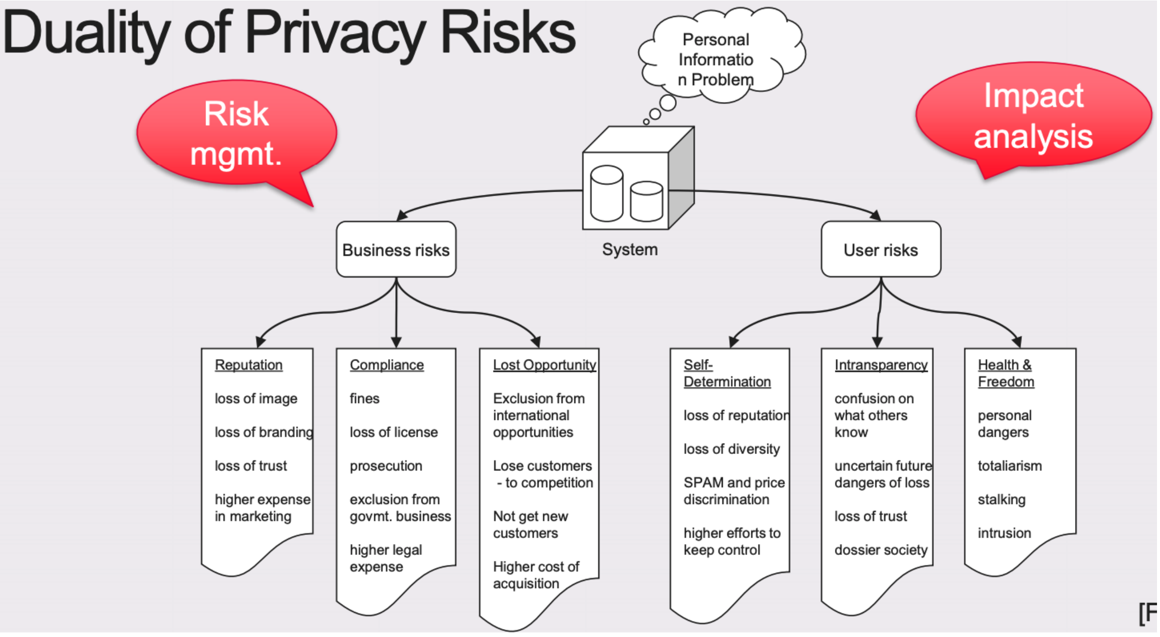
Likel / Imp	Negli	V low	Low	Med	High	V High	Extr
None	🟩	🟩	🟩	🟨	🟨	🟨	🟨
Minor	🟩	🟩	🟩	🟨	🟨	🟨	🟨
Med	🟨	🟨	🟨	🟨	🟨	🟨	🟨
High	🟨	🟨	🟨	🟨	🟥	🟥	🟥
V High	🟨	🟨	🟨	🟨	🟥	🟥	🟥
Extr	🟨	🟨	🟨	🟨	🟥	🟥	🟥

Three levels of risk are normally adequate: low, moderate, high

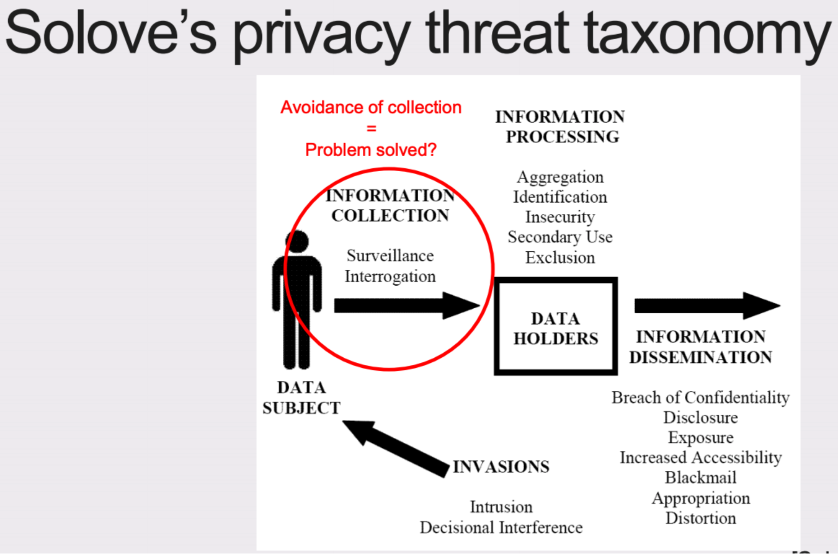
5.5 Risks to privacy

- Risks to the individual as a result of contravention of their rights in relation to privacy, or loss, damage, misuse or abuse of their personal information.
- Risks to the organization as a result of:

- perceived harm to privacy;
- a failure to meet public expectations on the protection of personal information;
- retrospective imposition of regulatory conditions;
- low adoption rates or poor participation in the scheme from both the public and partner organizations;
- the costs of redesigning the system or retro-fitting solutions;
- collapse of a project or completed system;
- withdrawal of support from key supporting organizations due to perceived privacy harms; and/ or
- failure to comply with the law, leading to:
- enforcement action from the regulator; or
- compensation claims from individuals.



Duality of Privacy Risks



Solove’s privacy threat taxonomy

5.5.1 Stakeholder: A persona with vulnerabilities

Background

- Streamer/Youtuber
- E-sports professional
- Has a following of more than 10 000 000
- 16-24 years old
- Female
- Uses an alias while being online

Technology expertise level

- High level of computer habit, but not a super user
- Have an good understanding of what could happen if information is leaked but not of how the attack would be performed

Technology use

- Consoles for gaming purposes
- Computer and phone for social networking

Access location

- Home network
- Public network

Threats from technology use

1. Reachable on electronic platforms for messaging
2. Traceable through game traffic.

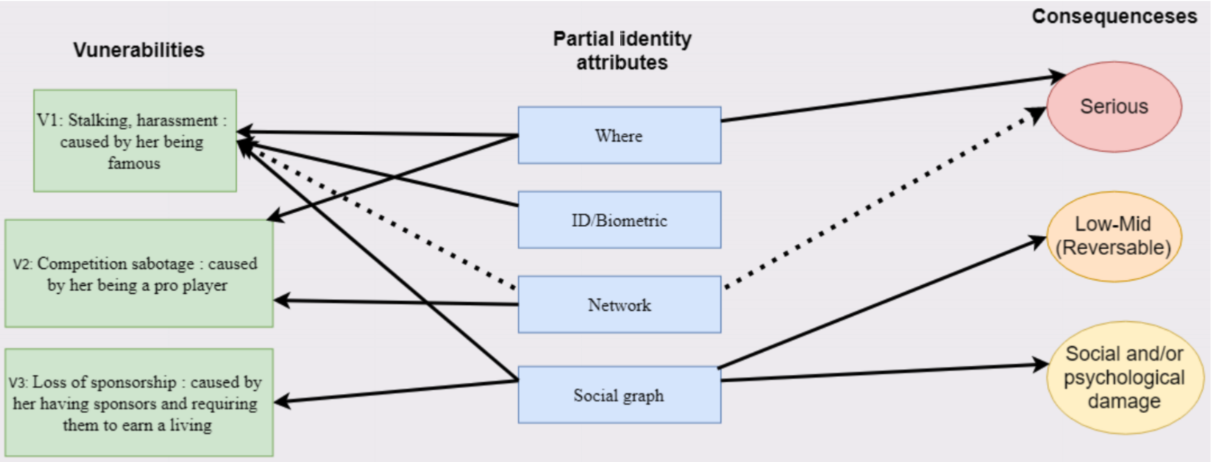
Vulnerabilities

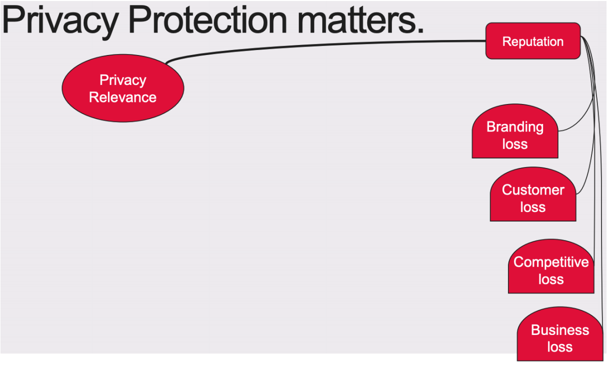
1. Stalking, harassment : caused by her being famous
2. Competition sabotage : caused by her being a pro player
3. Loss of sponsorship : caused by her having sponsors and requiring them to earn a living
   N.B for graph: Add one from ID to stalking, Add one from Network to Sabotage

Needs

- To be able to stay anonymous
- To not be spied upon
- For her career to continue.

5.5.2 Impact vs. Risk


Vunerabilities
Partial identity attributes
Consequenceses
V1: Stalking, harassment : caused by her being famous
V2: Competition sabotage : caused by her being a pro player
V3: Loss of sponsorship : caused by her having sponsors and requiring them to earn a living
Where
ID/Biometric
Network
Social graph
Serious
Low-Mid (Reversable)
Social and/or psychological damage



Privacy Protection matters.

Privacy Relevance

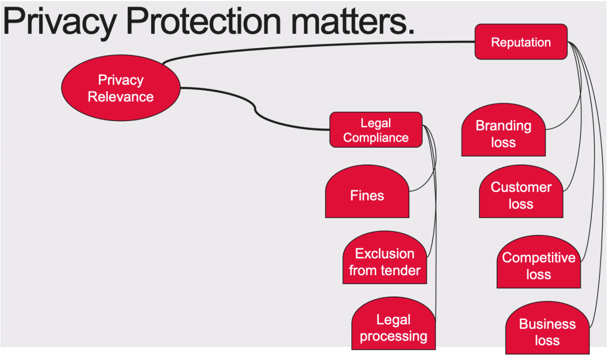
Reputation

Branding loss

Customer loss

Competitive loss

Business loss



Privacy Protection matters.

Privacy Relevance

Legal Compliance

Fines

Exclusion from tender

Legal processing

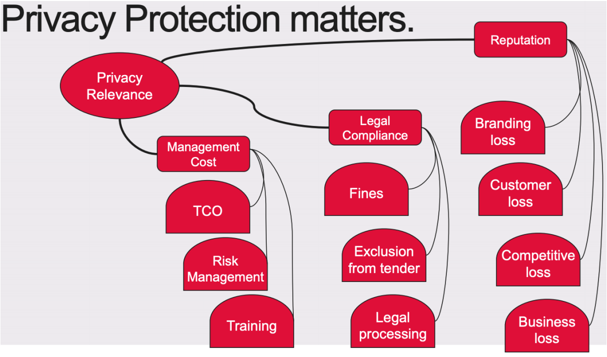
Reputation

Branding loss

Customer loss

Competitive loss

Business loss



Privacy Protection matters.

Privacy Relevance

Management Cost

TCO

Risk Management

Training

Legal Compliance

Fines

Exclusion from tender

Legal processing

Reputation

Branding loss

Customer loss

Competitive loss

Business loss

Problem with "cost per privacy breach"

- Who pays the cost?
- Risk management usually is used by service providers, system owners, or in general businesses to minimize their own losses.
- Customers' losses, and data subject's losses are not necessarily losses for the system owner.
- Regulation (laws and fines) are often used to align data subject losses with corporate losses in case of corporate misbehavior.

5.6 Drawbacks

- Lack of quantified data (cost & occurrence of incidents, effectivity & cost of PET)
  - Legislation on mandatory reporting and breaches
- Much "expert guessing" necessary
  - Good for expert's hourly rates
  - Bad for scientific accuracy
- Lack of long-term privacy risk model (duality!)
- Good for scientists:
  - More research necessary
  - More research funding?
  - Opportunities for master thesis work

5.7 Summary Privacy Risk Assessment

- Privacy management is part of IT management
- Some of the business implications are not well researched
- Many of the economic parameters of PET and their usage are unknown
- Privacy-enhancing technology is available
- Often, focus is on risks to service providers, not end users
- However, all stakeholders and their investments are threatened by risk.

6 Lecture 6: Privacy and Security Management

Overview

- Introduction to security and privacy management
- Case study / group work: Smart factory for smart cars
- Controls and risk treatment
- Incident handling

6.1 IT security management is a horizontal activity

- Part of quality management (product and service quality depend on IT quality)
- Part of operations management (IT runs production)
- Part of procurement (security requirements when sourcing cloud services)
- Part of HR management (planning, recruiting, training, dispatching of staff)
- Part of facility management (physical security of IT components)
- Part of logistics (both on way in and on way out)
- Part of sales (web shops, digital procurement)
- Part of finances (payment, billing, taxation, custome)

Most departments and functions will have contact with IT security management.

6.1.1 Stakeholders

The Players

- The Board
- The CEO
- The ISMS Forum: CTO, CSO, DPO, Management, Product owners

The Process

- Establish/Upgrade controls
- Reporting and Monitoring
- Continued evaluation
- Corrective actions

The Subjects

- Humans
- Assets
  - Equipment
  - Networks
  - Applications
  - Information Stores

The Documents

- Policy
- Procedures for handling
  - Assets
  - Incidents
  - People
- Detailed routines as appropriate

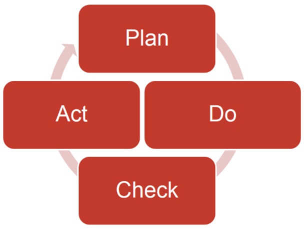
6.1.2 Organizing the ISMS

- Get management support & budget!
- Regular meetings (e.g. monthly) where incidents are analyzed and priorities get defined.
- Define triggers that cause re-assessment!
- Set up ISMS panel with participation of relevant roles:
  - Head of IT
  - Management
  - Head of Production
  - IT security managers

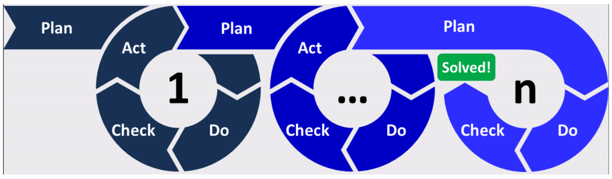
6.2 ISO 27000 security management

- A group of standard procedures and background documents.
- Unfortunately pay-for documents, even thought the Swedish state pays for writing them. We'll have to use excerpts(to take or select (a passage) from a book, article, etc.).
- Many organization train their staff in ISO27000, but do not aim for certification.
- Explains how security management works, how it is integrated into businesses, what it manages, and how risks and risk controls are found.
- An organization can get certified according to ISO27000 for complete and successful implementation of security management.

Continuous cyclic activity:



Continuous improvement over several rounds



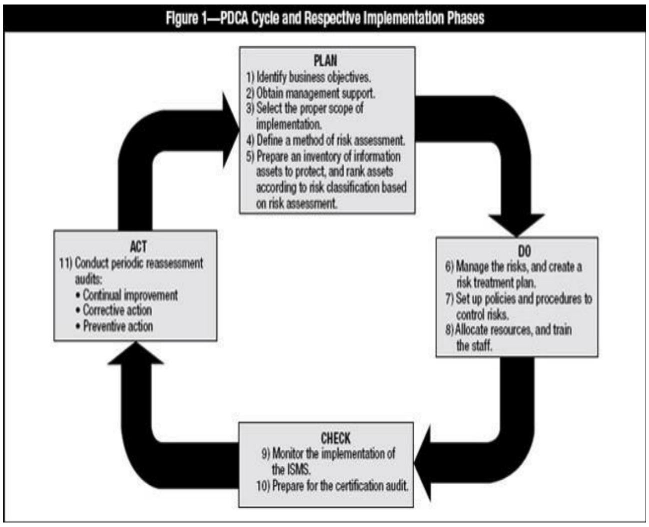


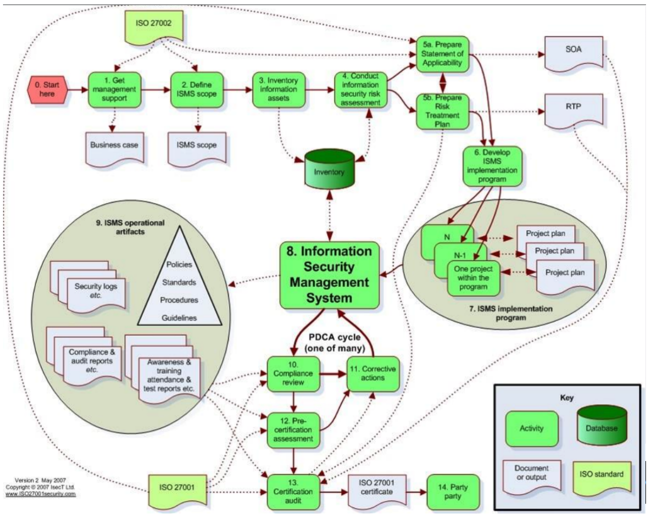
Figure 1—PDCA Cycle and Respective Implementation Phases

PLAN
1) Identify business objectives.
2) Obtain management support.
3) Select the proper scope of implementation.
4) Define a method of risk assessment.
5) Prepare an inventory of information assets to protect, and rank assets according to risk classification based on risk assessment.

DO
6) Manage the risks, and create a risk treatment plan.
7) Set up policies and procedures to control risks.
8) Allocate resources, and train the staff.

CHECK
9) Monitor the implementation of the ISMS.
10) Prepare for the certification audit.

ACT
11) Conduct periodic reassessment audits:
- Continual improvement
- Corrective action
- Preventive action


ISO 27002
0. Start here
1. Get management support
2. Define ISMS scope
3. Inventory information assets
4. Conduct information security risk assessment
5a. Prepare Statement of Applicability
5b. Prepare Risk Treatment Plan
SOA
RTP
Business case
ISMS scope
Inventory
6. Develop ISMS implementation program
9. ISMS operational artifacts
Policies
Standards
Procedures
Guidelines
Security logs etc.
Compliance & audit reports etc.
Awareness & training attendance & test reports etc.
8. Information Security Management System
N
N-1
One project within the program
Project plan
Project plan
Project plan
7. ISMS implementation program
PDCA cycle (one of many)
10. Compliance review
11. Corrective actions
12. Pre-certification assessment
13. Certification audit
ISO 27001
ISO 27001 certificate
14. Party party
Key
Activity
Database
Document or output
ISO standard
Version 2 May 2007
Copyright © 2007 IsecT Ltd.
www.ISO27001security.com

6.3 14 Domains of ISO27001:2013 Annex A

A.5 - Information security policies
A.6 - Organization of information security
A.7 - Human resource security
A.8 - Asset management
A.9 - Access control
A.10 - Cryptography
A.11 - Physical and environmental security
A.12 - Operations security
A.13 - Communications security
A.14 - System acquisition, development and maintenance
A.15 - Supplier relationships
A.16 - Information security incident management
A.17 - Information security aspects of business continuity management
A.18 - Compliance

6.3.1 Information Security Incident Management

A.16.1 - *Management of information security incidents and improvements*
A.16.1.1 - Responsibilities and procedures
A.16.1.2 - Reporting information security events
A.16.1.3 - Reporting information security weaknesses
A.16.1.4 - Assessment of and decision on information security events
A.16.1.5 - Response to information security incidents
A.16.1.6 - Learning from information security incidents
A.16.1.7 - Collection of evidence

6.3.2 Human Resources Security

A.7.1 - *Prior to employment*
A.7.1.1 - Screening
A.7.1.2 - Terms and conditions of employment
A.7.2 - *During employment*
A.7.2.1 - Management responsibilities
A.7.2.2 - Information security awareness, education and training
A.7.2.3 - Disciplinary process
A.7.3 - *Termination and change of employment*
A.7.3.1 - Termination or change of employment responsibilities

6.4 Triggers for re-assessment /new PDCA cycle

- Regular update (e.g. bi-annual)
- Internal changes in infrastructure
- New software installed
- New suppliers
- Major staff changes or other corporate events (layoffs, competence loss)
- Outsourcing to subcontractors
- Major software updates
- Changes in physical location
- Product updates or new products
- "World change": Newly discovered risks, hacking tools, attacks, crypto analysis

6.5 Finding controls for risks (case study)

6.5.1 Implementing controls

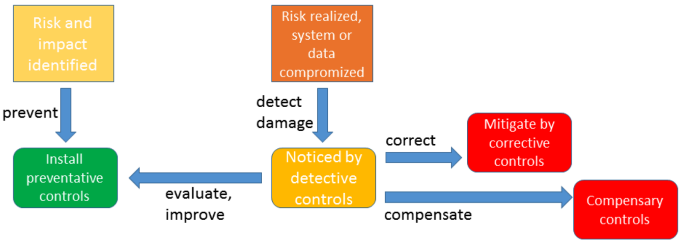
- Control selection based on identified risks.
- List-based specification of necessary controls.
- Selection and implementation of controls. **Remember: controls are technical or administrative!**
- See example control list and checklist: "MAPPING TO ISO 27001 CONTROLS"

6.5.2 Risk treatment

- Reduction of risk by using controls that mitigate risks.
- Controls are implemented into infrastructures, procedures and resources
- Controls are chosen from control lists (catalogs from standards)
- Technical controls - administrative controls

6.5.3 Security and privacy controls

- To reduce or remove a risk we chose appropriate controls that treat risks.
- Choose e.g. privacy controls. Example: NIST 800-53 and Privacy Overlay.

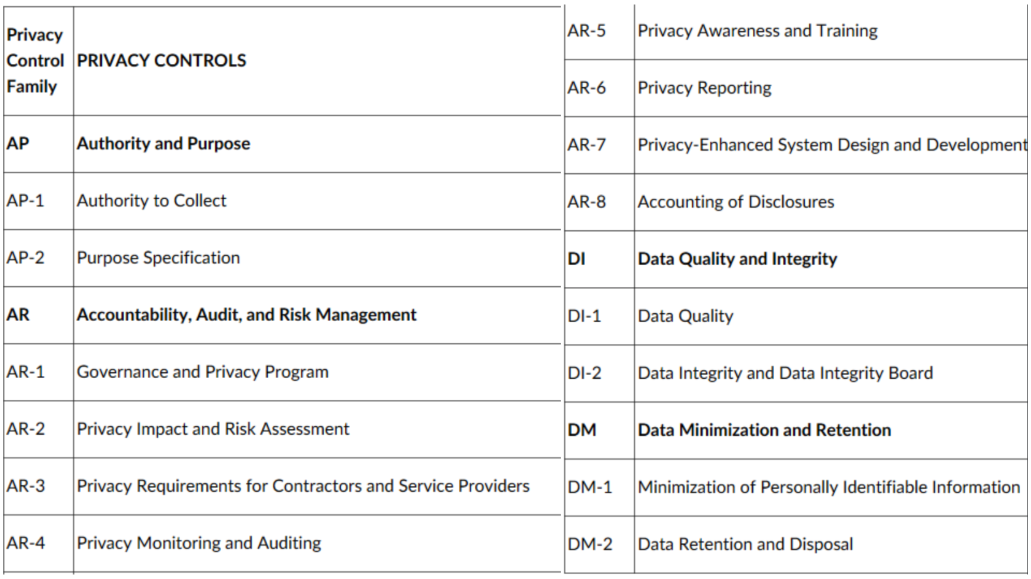

Risk and impact identified
prevent
Install preventative controls
Risk realized, system or data compromized
detect damage
Noticed by detective controls
evaluate, improve
correct
Mitigate by corrective controls
compensate
Compensary controls

6.5.4 NIST privacy controls

NIST draft Special Publication 800-53 on Security and Privacy Controls for Information Systems and Organizations is the specification of privacy and security controls for public offices in the United States. It contains an extensive collection of specified controls including appendices that show how to select controls that respond to various risk and impact levels. CNSS Privacy Overlays to NIST

On April 23, 2015, the Committee on National Security Systems (CNSS) published the Privacy Overlay to CNSS Instruction (CNSSI) 1253, "Security Categorization and Control Selection for National Security Systems." The Privacy Overlay is Appendix F, Attachment 6 to CNSSI 1253

The Privacy Overlay is comprised of four Privacy Overlays that identify security and privacy control specifications from NIST Special Publication (SP) 800-53, rev. 4 "Security and Privacy Controls for Federal Information Systems and Organizations" to protect personally identifiable information (PII), including protected health information (PHI), in National Security Systems (NSS) and reduce privacy risks to individuals throughout the information life cycle. It includes threat and impact specifications. $https://www.cnss.gov/CNSS/issuances/Instructions.cfm$

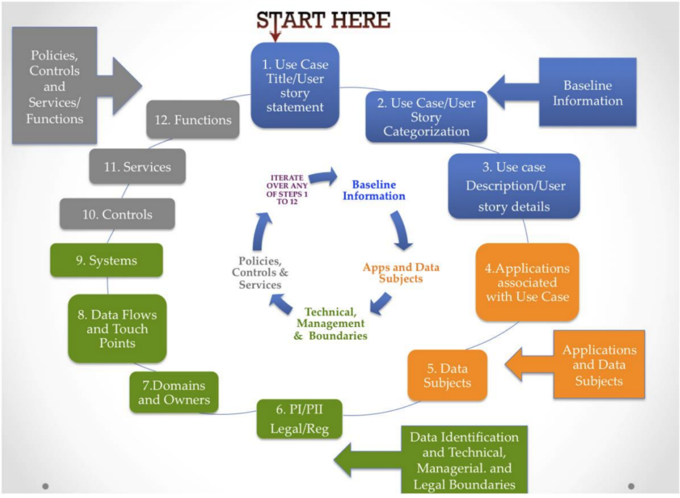


Privacy Control Family	**PRIVACY CONTROLS**
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-6	Privacy Reporting
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal

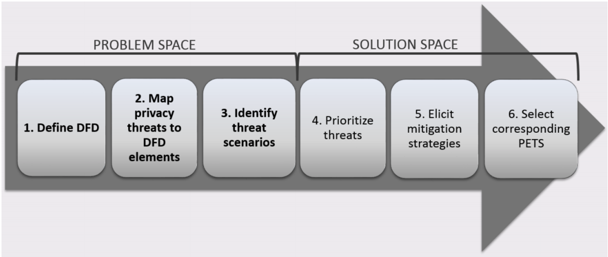
12-step process for "privacy by Design"

- OASIS method
- Is a PDCA cycle
- Includes risk analysis

From **OASIS Privacy by Design Documentation for Software Engineers** (PbD-SE)

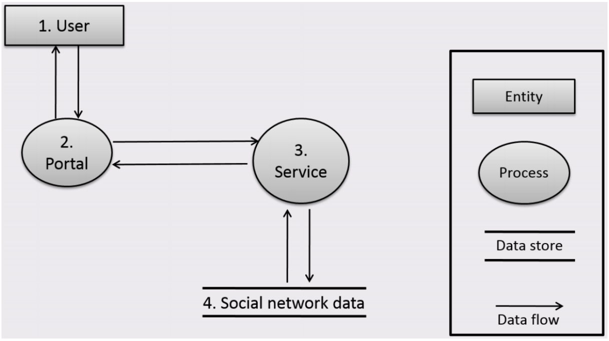

START HERE
Policies, Controls and Services/ Functions
1. Use Case Title/User story statement
2. Use Case/User Story Categorization
Baseline Information
3. Use case Description/User story details
4.Applications associated with Use Case
Applications and Data Subjects
5. Data Subjects
Data Identification and Technical, Managerial. and Legal Boundaries
6. PI/PII Legal/Reg
7.Domains and Owners
8. Data Flows and Touch Points
9. Systems
10. Controls
11. Services
12. Functions
ITERATE OVER ANY OF STEPS 1 TO 12
Baseline Information
Apps and Data Subjects
Technical, Management & Boundaries
Policies, Controls & Services

6.6 LINDDUN


PROBLEM SPACE
SOLUTION SPACE
1. Define DFD
2. Map privacy threats to DFD elements
3. Identify threat scenarios
4. Prioritize threats
5. Elicit mitigation strategies
6. Select corresponding PETS

LINDDUN.org

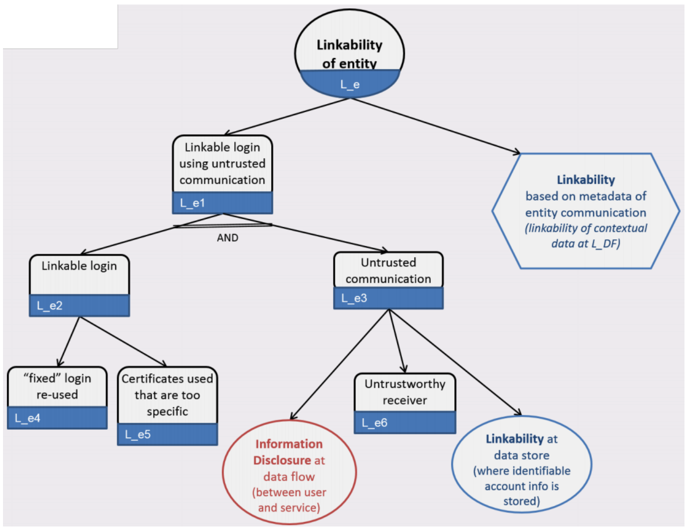
6.6.1 Data flow diagram



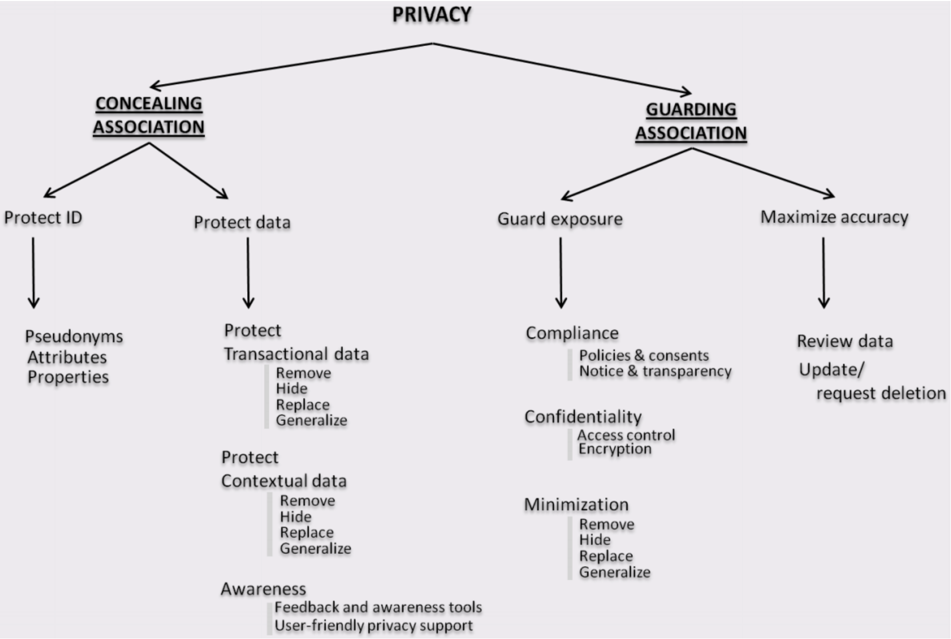
6.6.2 Threat trees

Threat categories:

- **L**inkability,
- **I**dentifiability,
- **N**on-repudiation,
- **D**etectability,
- **D**isclosure of information,
- **U**nawareness,
- **N**on-compliance


Linkability of entity
L_e
Linkable login using untrusted communication
L_e1
AND
Linkability based on metadata of entity communication (linkability of contextual data at L_DF)
Linkable login
L_e2
Untrusted communication
L_e3
"fixed" login re-used
L_e4
Certificates used that are too specific
L_e5
Untrustworthy receiver
L_e6
Information Disclosure at data flow (between user and service)
Linkability at data store (where identifiable account info is stored)

6.6.3 Mitigation



6.7 Threat intelligence as input for risk assessment

- CERT services: Supranational, national, sector-wide, intra-organizational
- Reports from government security authorities, industry, academy, insurance industry
- Commercial data sources (examples): *https : //breachlevelindex.com/*

  Gardner webroot: *https : //www.gartner.com/imagesrv/media − products/pdf/webroot/issue1_webroot.pdf*

  McAffee threat intelligence exchange:

  https : //www.mcafee.com/enterprise/en − us/products/threat − intelligence − exchange.html

- Mandatory reporting & publishing duties, e.g. privacy breaches:

  http : //www.informationisbeautiful.net/visualizations/worlds − biggest − data − breaches − hacks/

6.8 Cost of information security incidents

- Examples from ENISA report on cost of incidents
- Privacy breaches and their cost
- Effect of various security measures

Figure 6: Average annualized cost by industry sector (millions) [16]

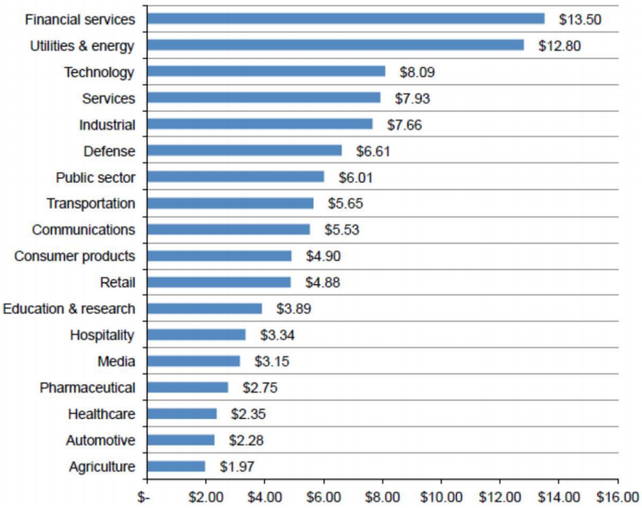


Figure 9: Percentage annualized cybercrime cost, by attack type [16]

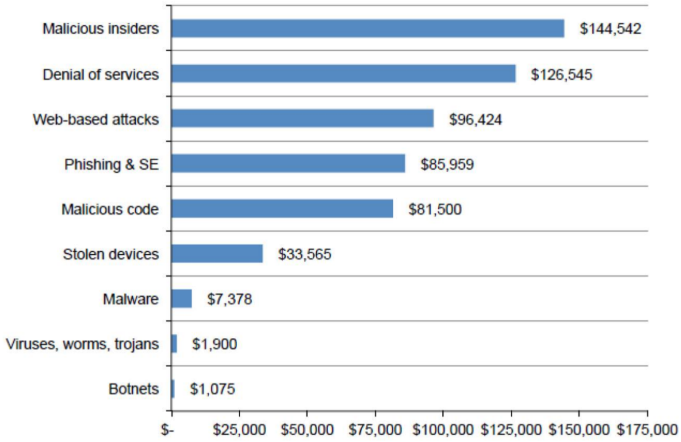


Figure 8: Attack/Threat types per CII sector (graphical view of Table 2)

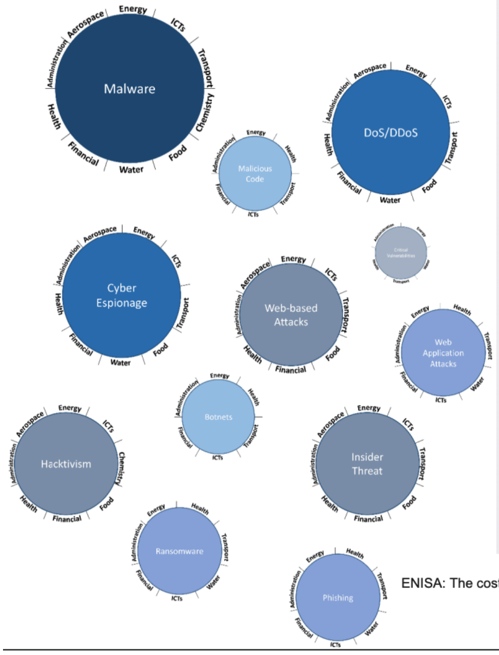
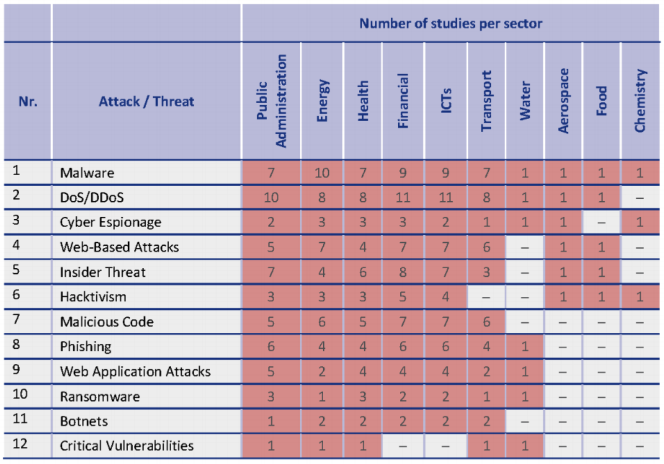


Table 2: Attack/Threat types per CII sector



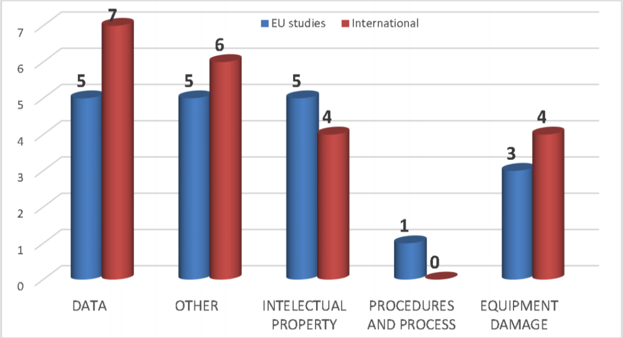
		Number of studies per sector									
Nr.	Attack / Threat	Public Administration	Energy	Health	Financial	ICTs	Transport	Water	Aerospace	Food	Chemistry
1	Malware	7	10	7	9	9	7	1	1	1	1
2	DoS/DDoS	10	8	8	11	11	8	1	1	1	–
3	Cyber Espionage	2	3	3	3	2	1	1	1	–	1
4	Web-Based Attacks	5	7	4	7	7	6	–	1	1	–
5	Insider Threat	7	4	6	8	7	3	–	1	1	–
6	Hacktivism	3	3	3	5	4	–	–	1	1	1
7	Malicious Code	5	6	5	7	7	6	–	–	–	–
8	Phishing	6	4	4	6	6	4	1	–	–	–
9	Web Application Attacks	5	2	4	4	4	2	1	–	–	–
10	Ransomware	3	1	3	2	2	1	1	–	–	–
11	Botnets	1	2	2	2	2	2	–	–	–	–
12	Critical Vulnerabilities	1	1	1	–	–	1	1	–	–	–

ENISA: The cost of incidents affecting CIIs, 2016

UiO : University of Oslo

KARLSTAD UNIVERSITY

Figure 10: Assets affected



Example: Business-side cost factors of privacy management

Privacy Office: Costs associated with dedicated staff, office overhead, travel and business equipment.
Policy & Procedures: Costs associated with the creation, review, publication and dissemination of the privacy policy (and privacy notice when applicable).
Downstream Communications: Costs associated with the communication and outreach activities for the privacy program both within the company and to outside stakeholders.
Training & Awareness: Costs associated with the education of employees and other key company stakeholders about the privacy policy, program and related concepts.
Enabling Technologies: Costs associated with technologies that help mitigate privacy risk, enhance responsible information management, or protect the critical data infrastructure.
Employee Privacy: Costs associated with the protection of sensitive employee records, including heath care and OSHA claims.
Legal Activities: Costs associated with legal review and counsel concerning the privacy program as well as legal defence costs in the event of a privacy violation.
Audit & Control: Costs associated with the monitoring, verification and independent audit of the privacy program, including use of controlled self-assessment tools.
Redress & Enforcement: Costs incurred to provide upstream communication of a privacy or data protection breach to appropriate parties within the organization, including the cost of investigation and collaboration with law enforcement. In addition to the above cost center activities, the current research captured additional information

Figure 5. Per capita cost by industry classification
*Historical data are not available for all years
Measured in US$

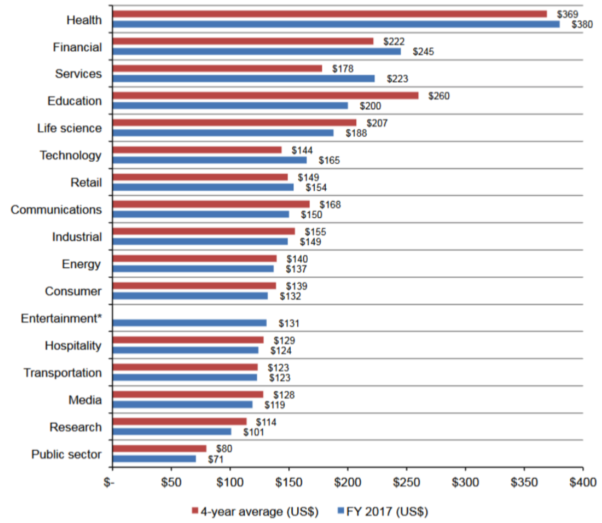
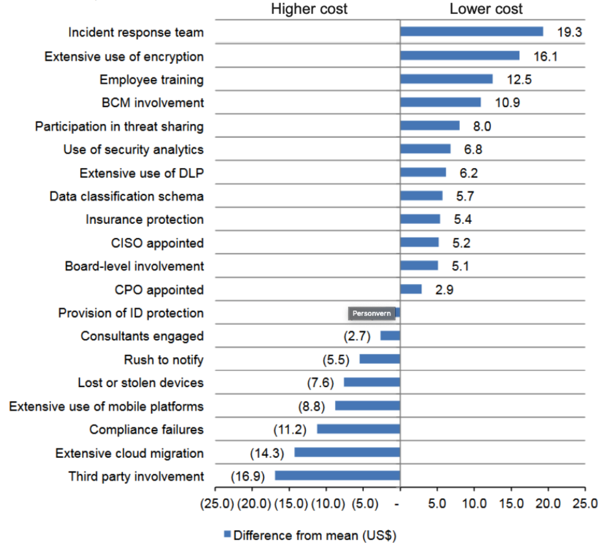


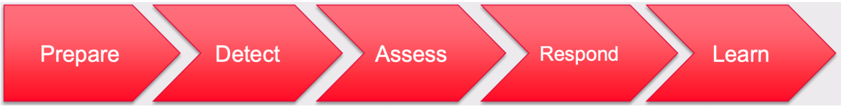
Figure 9. Impact of 20 factors on the per capita cost of data breach
Measured in US$



6.9 Incident management: Definitions in ISO 27000

- Information security incident: An information security incident is made up of one or more unwanted or unexpected information security events that could possibly compromise the security of information and weaken or impair business operations.

- Information security incident management: Information security incident management is a set of processes that organizations use to deal with information security incidents. It includes a detection process, a reporting process, an assessment process, a response process, and a learning process.



Prepare Detect Assess Respond Learn

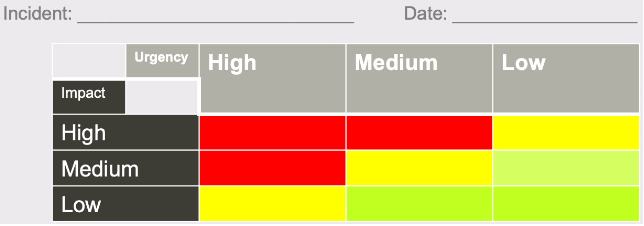
Incident management cycle

6.9.1 Incident management

1. **Plan and prepare**: establish an information security incident management policy, form an Incident Response Team etc.
2. **Detection and reporting**: someone has to spot and report "events" that might be or turn into incidents;
3. **Assessment and decision**: someone must assess the situation to determine whether it is in fact an incident;
4. **Responses**: contain, eradicate, recover from and forensically analyze the incident, where appropriate;
5. **Lessons learned**: make systematic improvements to the organization's management of information risks as a consequence of incidents experienced.

6.9.2 Incident classification

https : //www.iso27001security.com/html/27035.html



Incident: ______________________ Date: ______________

Impact \ Urgency	High	Medium	Low
High	🟥	🟥	🟨
Medium	🟥	🟨	🟩
Low	🟨	🟩	🟩

Classify and prioritize by assessing impact and urgency, then order all ”red” Incidents according to company priorities (security policy, production, etc.).

Ponemon Institute, "2017 Cost of Breach Study" - Global Overview", 2017

6.9.3 Preparation of incident management

1. Establish information security incident management policy
2. Update information security and risk management policies
3. Create information security incident management plan
4. Establishing an Incident Response Team (CERT – Computer Emergency Response Team or CSIRT – Computer Security Incident Response Team)
5. Define technical and other support
6. Create information security incident awareness and training
7. Test and exercise the information security incident management plan
8. Document lesson learnt

ISO/IEC 27035-2:2016 Guidelines to plan and prepare for incident response

6.9.4 Summary of incident and risk management

- Incident management understands, contains and recovers from security incidents
- Incident management demands experts, resources and preparation
- Treatment of risks and their impact is an extensive process changing infrastructure and processes with controls that demands preparation, resources, knowledge and priority in corporate information security management.

Resource problem for smaller companies. Recommendation:

- Minimize IT complexity and personal data collection to the bare necessities.
- Stick to a particular purpose – more flexibility creates more complexit.
- Establish relationship with emergency response firms BEFORE incident happens.

6.10 Summary

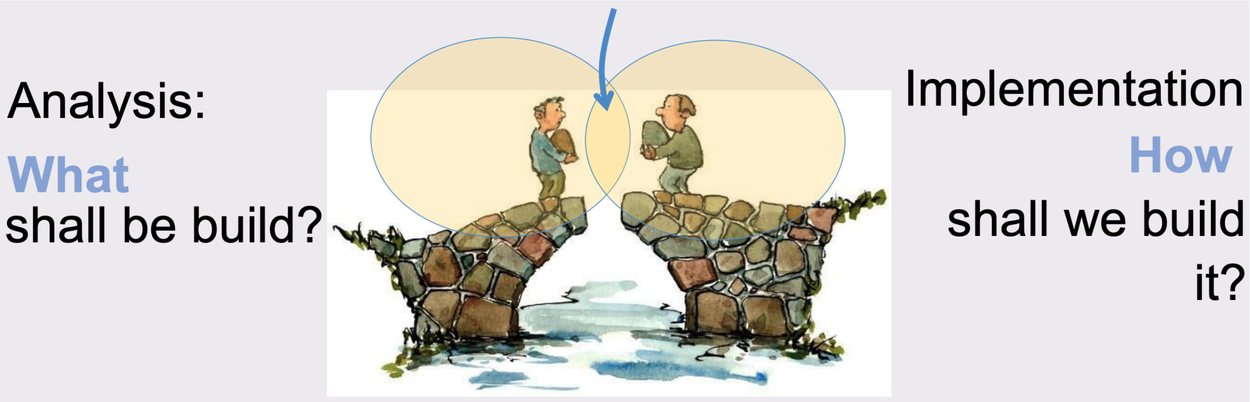
- IT security and privacy management manages risks related to data and systems.
- Risks cause disruption, direct cost and risk handling cost.
- IT security and privacy management is a complex process that involves many parts of an organization, their suppliers and the basic communication and IT infrastructures they use.
- Personal data is a special class of information assets that must be a part of the security management process. Many privacy controls are ADMINISTRATIVE!
- Production or delivery of services is critically dependent on IT.
- IT security investments are investments that pay off by preventing and reducing incident cost.

7 Lecture 7: Privacy Engineering

Overview

- Software architecture
- Privacy Design strategies and tactics
- Privacy Patterns
- Dark Privacy Patterns

7.1 Architecting & Designing



Analysis:
What
shall be build?

Implementation
How
shall we build
it?

7.2 Attempts to define software architecture

Many definitions.

Many definitions similar to IEEE standard 1471:

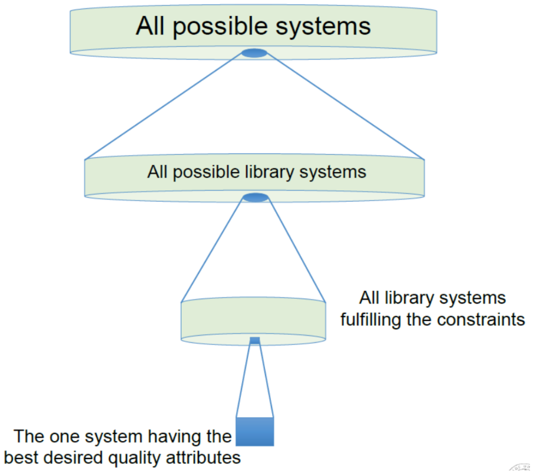
"the fundamental organization of a system embodied in its components, their relationships to each other and to the environment and the principles guiding its design and evolution."

7.2.1 What is Software quality?

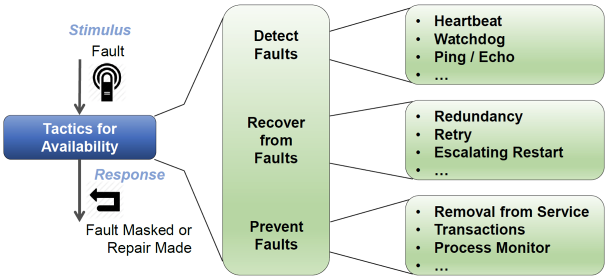
- Latin "qualitas": the nature/distinguishing characteristic of something
- Quality: "the degree of excellence of something"
- Quality attributes reflect the multiple dimensions of quality:
- A software can be great w.r.t. performance...and pretty bad w.r.t. maintainability
- Quality attributes are categorized and refined in quality models
- ISO 25010 defines a quality model with eight top level attributes
- Functional Suitability
- Performance Efficiency
- Compatibility
- Usability
- Reliability
- Security
- Maintainability
- Portability

7.2.2 What is driving the software architecture the most?

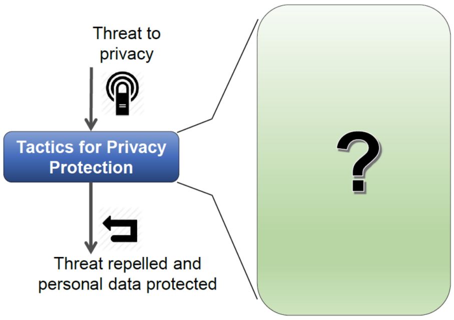
- Functional requirements?
  - Naah, any structure will do.
- Constraints?
  - Often imply quite easy design decisions
- Quality attribute requirements?
  - Most important drivers
  - Often competing and requiring trade-offs


All possible systems
All possible library systems
All library systems fulfilling the constraints
The one system having the best desired quality attributes

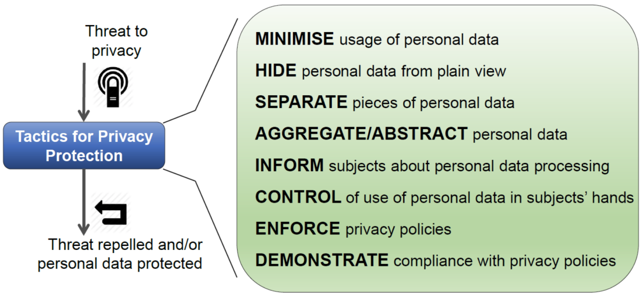
Example: Architectural tactics for availability



What we want to find out...


Threat to privacy
Tactics for Privacy Protection
Threat repelled and personal data protected
?

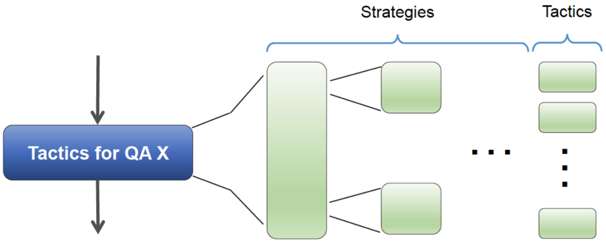
7.3 Overview of privacy design strategies


Threat to privacy
Tactics for Privacy Protection
Threat repelled and/or personal data protected

MINIMISE usage of personal data
HIDE personal data from plain view
SEPARATE pieces of personal data
AGGREGATE/ABSTRACT personal data
INFORM subjects about personal data processing
CONTROL of use of personal data in subjects' hands
ENFORCE privacy policies
DEMONSTRATE compliance with privacy policies

Strategies = Tactics?(!)

- Confusing terminology from two different communities:
  - Privacy design strategies from the privacy and security research community
  - Architecture tactics for privacy protection from the software architecture community
- We use them synonymously



7.3.1 Minimize

"The amount of personal data that is processed should be restricted to the minimal amount possible."

- Is the amount of personal data collected justified by the purpose?
- Is there another way of fulfilling the same purpose with less personal data?

Examples of implementation

- Use of pseudonyms in a system because there is no need for persons' real names

7.3.2 Hide

"Any personal data, and their relationships, should be hidden from plain view."

- Is personal data stored/transported/etc "as it is”"or is it, in some way, transformed such that it cannot easily be used by others
- Data in plain view is easier to abuse
- Who the "others" are, depends on the usage context

Examples of implementation

- Anonymization or encryption of data

7.3.3 Separate

"Personal data should be processed in a distributed fashion, in separate compartments whenever possible."

- Makes it harder to create full profiles of persons based on their personal data
- Prefer distributed processing over centralized processing
- Prefer local processing over remote processing

Examples of implementation

- Storing customer contact information and purchase information in separate databases

7.3.4 Aggregate/Abstract

"Personal data should be processed at the highest level of aggregation and with the least possible detail in which it is still useful."

- Process personal data at the level of detail that is absolutely necessary (and not in more detail)
- Aggregate data over groups of individuals, over groups of attributes, over time, ...

Examples of implementation

- Age ranges or regional categories instead of birthday and address in surveys

7.3.5 Inform

"Data subjects should be adequately informed whenever personal data is processed."

Inform data subjects about

- Which of their personal data is processed by which means for which purpose
- The security mechanisms used to protect their personal data
- Third parties with which data is shared
- Their data access rights

Examples of implementation

- Provide a clear, understandable privacy policy

7.3.6 Control

"Data subjects should be provided agency over the processing of their personal data."

- Provide appropriate means to data subjects to exert their data protection rights
- Provide appropriate means to data subjects for deciding whether or not to use a system and for controlling the processing of personal data

Examples of implementation

- Notifications of desired access rights of apps
- Customizable privacy settings in, e.g., social network systems
- Means to execute subjects' right to be forgotten

7.3.7 Enforce

"A privacy policy compatible with legal requirements should be in place and should be enforced."

- Create, maintain, and update a privacy policy
- A privacy policy accounts for technical controls and organizational controls to privacy protection
- It should cover the full lifecycle of a system

Example of implementation

- Access control systems

7.3.8 Demonstrate

"The data controller must be able to demonstrate compliance with the privacy policy and any legal requirement."

- Be always able to show how the privacy policy in place is implemented
- Explicitly required by the GDPR!

Example of implementation

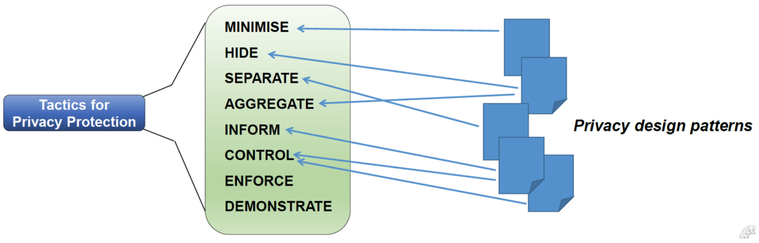
- Publish a recent audit certificate confirming compliance

7.4 Privacy Design Patterns

7.4.1 Description of patterns

- Name
- Context: The situation/class of system in which the pattern can be applied
- Problem: Description of what the pattern tries to solve, often express as the forces that it tries to balance
- Solution: description of the structure, i.e. configuration of elements that solves the problem and how they interact
- Often added categories
  - Summary of pattern
  - Goals: what is achieved by applying the patterns
  - Constraints and consequences: which benefits and potential disadvantages has the patterns
  - Motivating example
  - Known uses.

What are privacy design patterns?
According to the previous definition: a general, ***reusable software design solution*** to a ***common privacy protection problem*** within a given context.

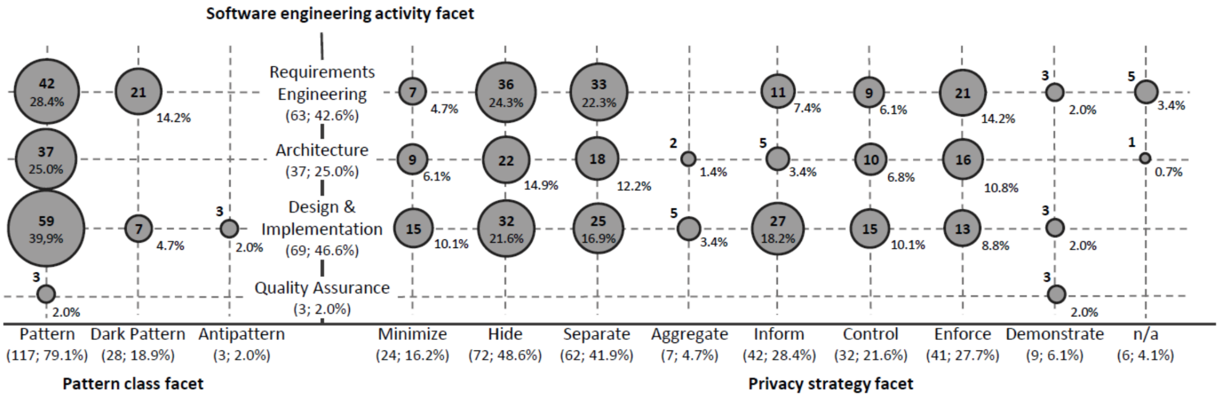

Tactics for Privacy Protection

MINIMISE
HIDE
SEPARATE
AGGREGATE
INFORM
CONTROL
ENFORCE
DEMONSTRATE

7.4.2 Location Granularity

- Context: A service collecting location data about a user.
- Problem
  - Many services require location-based data
  - Too much location information may harm user's privacy
- Solution
  - Introduce different levels of precision of geographical data
  - Choose most coarse-grained level
- Example
  - Weather app might still be precise enough based on ZIP-based location
- Applied strategy
  - Abstract

7.4.3 Survey of privacy design patterns



Survey of pattern literature. Snowballing, resulting classified set: 49 articles.

Lenhard, J., Fritsch, L., & Herold, S. (2017, August). A literature study on privacy patterns research. In 2017 43rd Euromicro Conference on Software Engineering and Advanced Applications (SEAA) (pp. 194-201). IEEE.

7.5 Dark Patterns - implementing the dark side

What are privacy dark patterns?

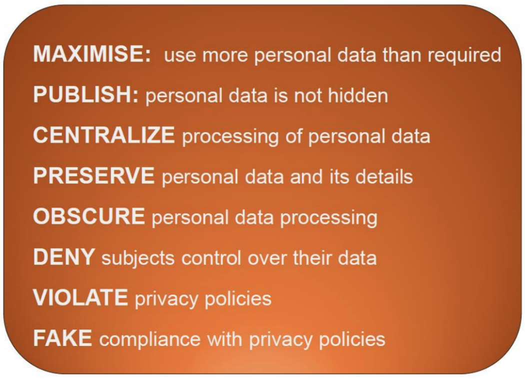
- **Recap:** privacy patterns are general, ***reusable software design solutons*** to ***common privacy protection problems*** within a given context.
- Privacy dark patterns are general, recurring software design solutions that constitute ***common privacy "infringements"*** within a given context.
- Not to be confused with anti-patterns

7.5.1 Forced registration

- **Context:** Any service technically *not* requiring personal accounts
- **Description:**
  - User wants to use some functionality that is only accessible after registration
  - The registration is technically unnecessary but gives the service provider access to the user's personal data
- **Effect:**
  - Users register with service provider.
  - Allows provider to track user.
  - Sloppy configuration of privacy settings is likely.
- **Example:**
  - Numerous webshops

7.5.2 Dark strategies

Privacy design strategies vs Dark pattern strategies



MAXIMISE: use more personal data than required

PUBLISH: personal data is not hidden

CENTRALIZE processing of personal data

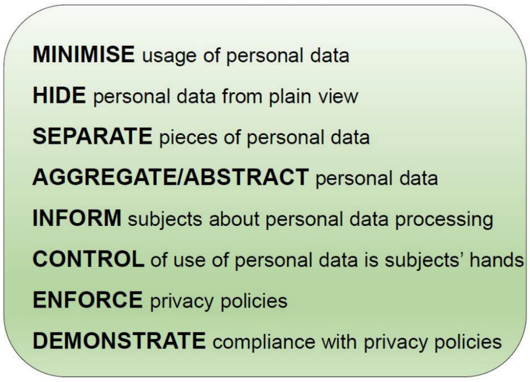
PRESERVE personal data and its details

OBSCURE personal data processing

DENY subjects control over their data

VIOLATE privacy policies

FAKE compliance with privacy policies



MINIMISE usage of personal data

HIDE personal data from plain view

SEPARATE pieces of personal data

AGGREGATE/ABSTRACT personal data

INFORM subjects about personal data processing

CONTROL of use of personal data is subjects' hands

ENFORCE privacy policies

DEMONSTRATE compliance with privacy policies

7.5.3 Survey excerpt: Privacy dark patterns

- Privacy Zuckering
- Bad Defaults
- Forced Registration
- Hidden Legalese Stipulations
- Immortal Accounts
- Address Book Leeching
- Shadow User Profiles.

Three of these dark patterns are directly related to identity management: Forced Registration, Address Book Leeching, and Shadow User Profiles.

7.6 Pattern collection method

- Patterns have been observed while using social media platforms and while surfing the web through TOR.
- Access through TOR browser, alternative access with Internet Explorer to determine TOR discrimination tactics' presence.

Published in: Fritsch, L. (2017). Privacy dark patterns in identity management. In Open Identity Summit (OID), 5-6 october 2017, Karlstad, Sweden. (pp. 93-104). Gesellschaft für Informatik.

7.6.1 Privacy dark pattern 1: Fogging identification with security

Summary: While asking for identity attributes, the requesting data collector obscures the purpose of the acquisition of additional identity attributes by claiming increased security for the contributing user.

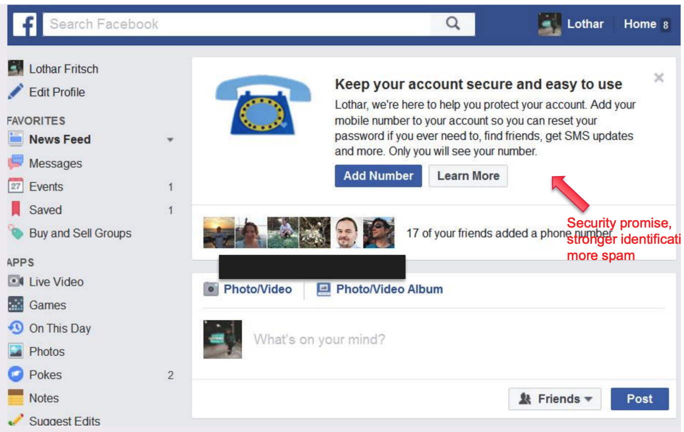
Context: On-line social media, apps, and general on-line services with user profiles or user accounts deploy this dark pattern.

Examples/Known Uses: This dark pattern has frequently been seen when logging into services provided by Google and by Facebook. It has been seen on LinkedIn and other social media.

Related Patterns: Forced registration, shadow user profiles.

Strategies: MAXIMIZE, CENTRALIZE, OBSCURE.

Countermeasures: Ignore request, skip, enter fake data, provide honeypot data, use obfuscation tools.



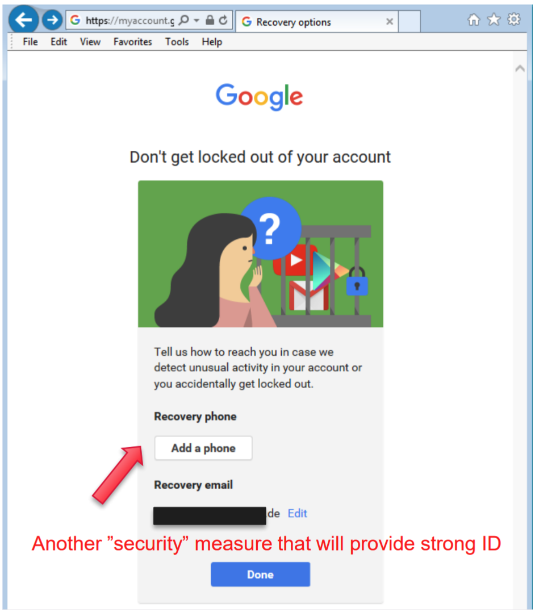
Keep your account secure and easy to use

Lothar, we're here to help you protect your account. Add your mobile number to your account so you can reset your password if you ever need to, find friends, get SMS updates and more. Only you will see your number.

17 of your friends added a phone number

[redacted]

Security promise, stronger identificati more spam



Don't get locked out of your account

Tell us how to reach you in case we detect unusual activity in your account or you accidentally get locked out.

Recovery phone

Recovery email

[redacted]de

Another "security" measure that will provide strong ID

7.6.2 Privacy dark pattern 2: Sweet seduction

Summary: On-line services ask for additional personal data that is not necessary to interact with the service. The requested data is promised to remain "invisible", or alternatively to remain governed by end user policy. The newly entered information is used to amend user profiles, and to pursue more targeted business (which is not mentioned on the collection screen).

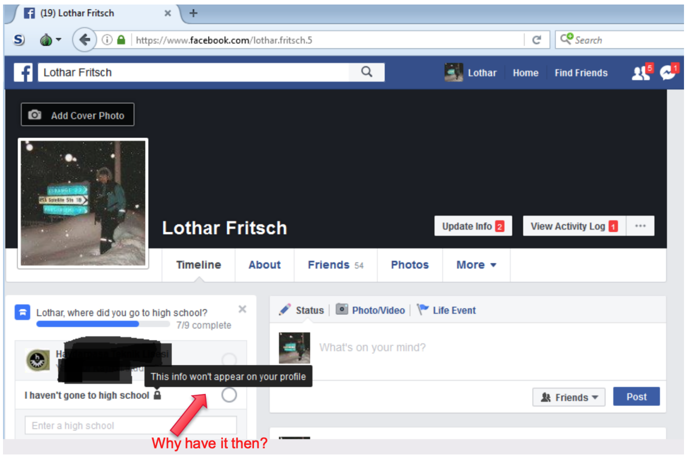
Context: The pattern has been observed as part of on-line social media that base their user identity management on profiles that collect identity attributes.

Examples/Known Uses: Facebook frequently applies the Sweet seduction pattern. Users are motivated to reveal their school information to Facebook while being promised that the information remains invisible. Upon requesting verified phone numbers, Facebook promises the user governance of how the phone number is used with an opt-out model.

Related Patterns: Privacy Zuckering, shadow user profiles.

Strategies: CENTRALIZE, OBSCURE, MAXIMIZE, PUBLISH

Countermeasures: Refuse data entry, provide fake data.



Lothar, where did you go to high school?
7/9 complete

[redacted]

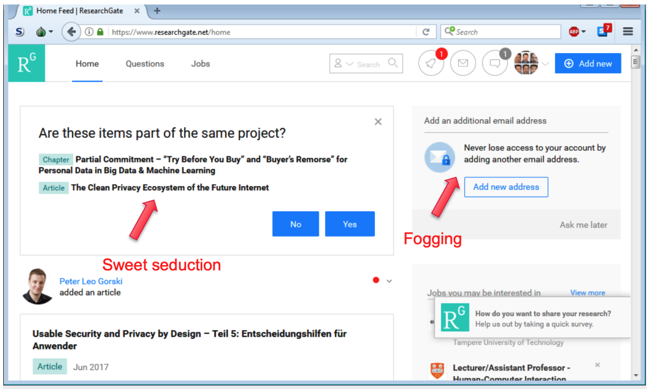
This info won't appear on your profile

I haven't gone to high school

Enter a high school

What's on your mind?

Why have it then?



Are these items part of the same project?

Chapter Partial Commitment – "Try Before You Buy" and "Buyer's Remorse" for Personal Data in Big Data & Machine Learning

Article The Clean Privacy Ecosystem of the Future Internet

No Yes

Sweet seduction

Peter Leo Gorski added an article

Usable Security and Privacy by Design – Teil 5: Entscheidungshilfen für Anwender

Article Jun 2017

Add an additional email address

Never lose access to your account by adding another email address.

Add new address

Ask me later

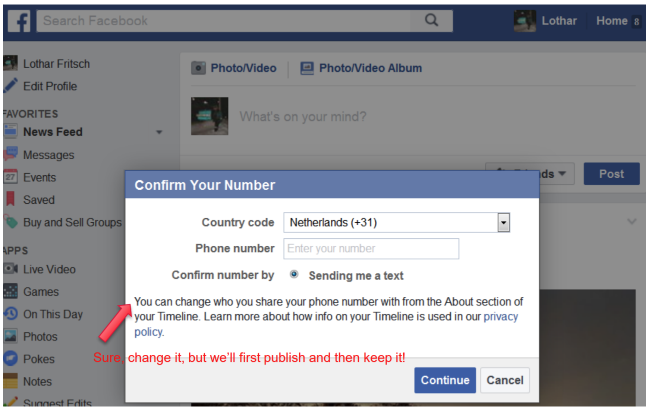
Fogging

Jobs you may be interested in View more

How do you want to share your research? Help us out by taking a quick survey.

Tampere University of Technology

Lecturer/Assistant Professor - Human-Computer Interaction



Confirm Your Number

Country code Netherlands (+31)

Phone number Enter your number

Confirm number by ● Sending me a text

You can change who you share your phone number with from the About section of your Timeline. Learn more about how info on your Timeline is used in our privacy policy.

Sure, change it, but we'll first publish and then keep it!

Continue Cancel

7.6.3 Privacy dark pattern 3: You can run but you can't hide.

Summary: Access to services is denied based on the fact that the accessing IP address is a known TOR exit node. The reason for denial is provided, or random error messages are given. Occasional multi-factor authentication is requested.

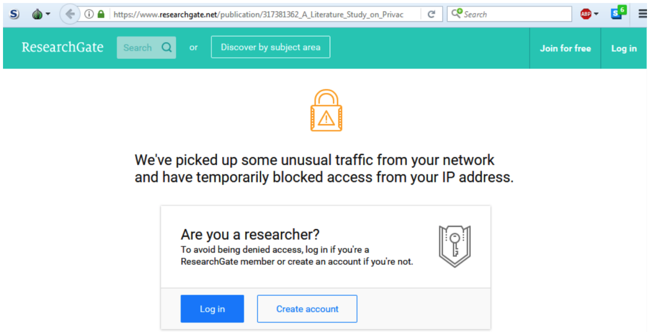
Context: This dark pattern is observed with e-commerce web sites, government web sites, payment web sites, blog web sites and many other on-line service providers.

Examples/Known Uses: Numerous examples collected. Among them Google, Skype, the European Union and SAP.

Related Patterns: -

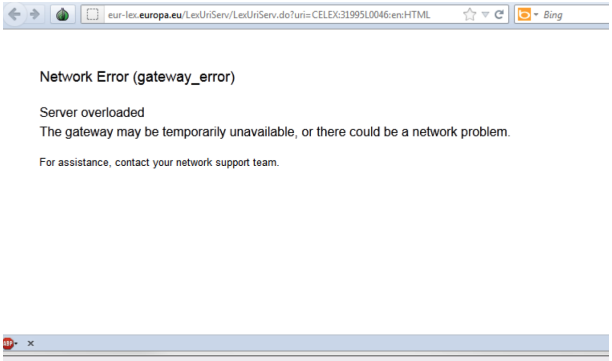
Strategies: DENY, MAXIMIZE.

Countermeasures: Use different anonymizer, VPN service, revert to paper-based business transactions to generate cost, boycott service. Complain to business managers about denied service.



We've picked up some unusual traffic from your network and have temporarily blocked access from your IP address.

Are you a researcher?
To avoid being denied access, log in if you're a ResearchGate member or create an account if you're not.

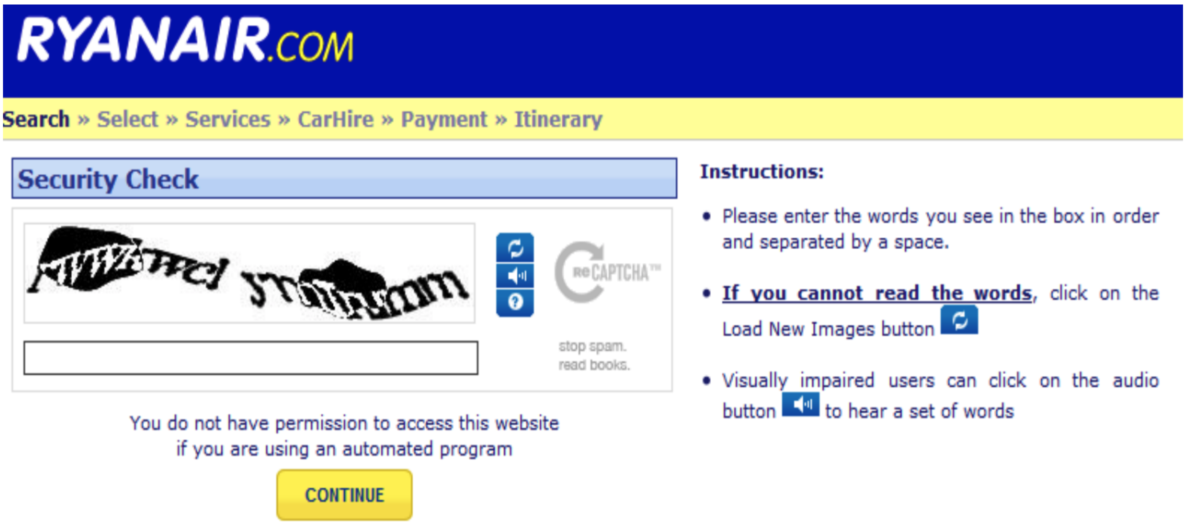

eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
Bing

Network Error (gateway_error)

Server overloaded
The gateway may be temporarily unavailable, or there could be a network problem.

For assistance, contact your network support team.

Not permitted to look at the EU data protection directive using an anonymizer, 5-Jul-2012, 11:36



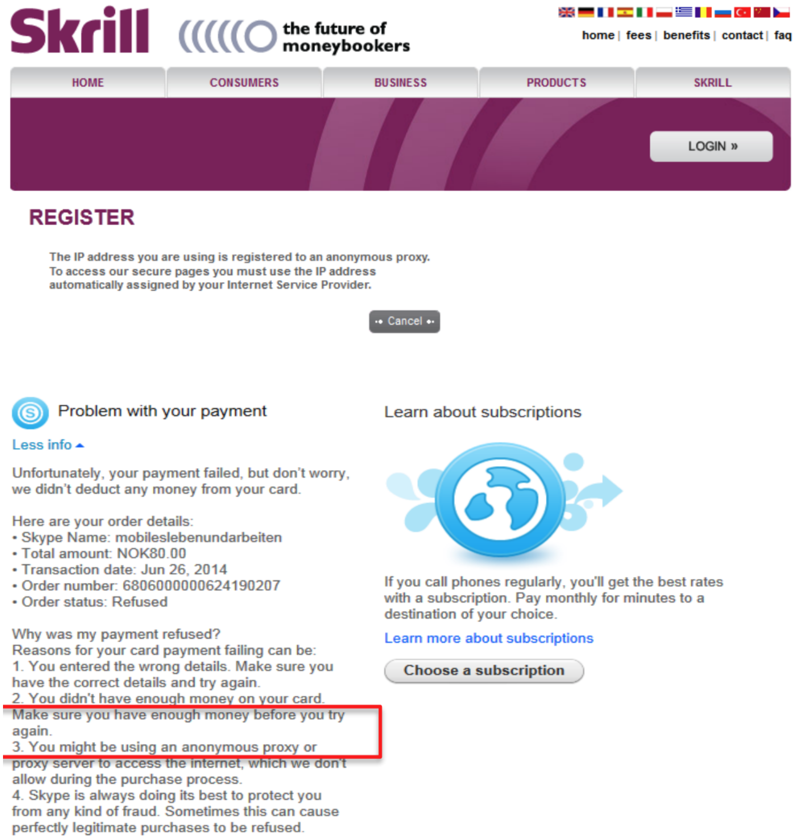
Security Check

You do not have permission to access this website if you are using an automated program

Instructions:

- Please enter the words you see in the box in order and separated by a space.
- **If you cannot read the words**, click on the Load New Images button
- Visually impaired users can click on the audio button to hear a set of words

Impossible captcha, 29-Aug-2012, 10:55



Skrill
the future of moneybookers
home | fees | benefits | contact | faq
HOME
CONSUMERS
BUSINESS
PRODUCTS
SKRILL
LOGIN »

REGISTER

The IP address you are using is registered to an anonymous proxy. To access our secure pages you must use the IP address automatically assigned by your Internet Service Provider.

Problem with your payment

Unfortunately, your payment failed, but don't worry, we didn't deduct any money from your card.

Here are your order details:

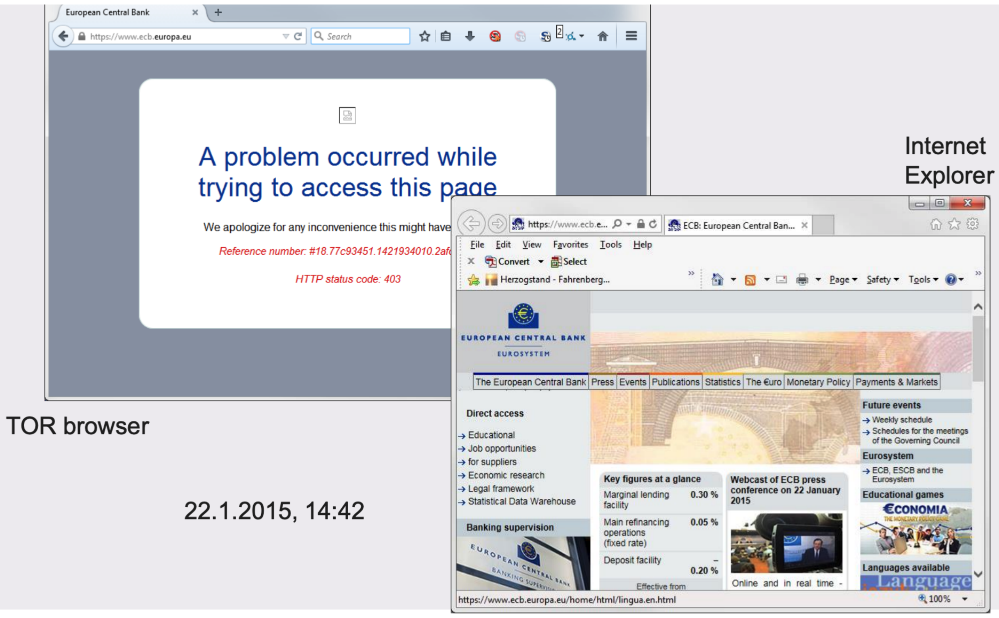
- Skype Name: mobileslebenundarbeiten
- Total amount: NOK80.00
- Transaction date: Jun 26, 2014
- Order number: 6806000000624190207
- Order status: Refused

Why was my payment refused?
Reasons for your card payment failing can be:
1. You entered the wrong details. Make sure you have the correct details and try again.
2. You didn't have enough money on your card. Make sure you have enough money before you try again.
3. You might be using an anonymous proxy or proxy server to access the internet, which we don't allow during the purchase process.
4. Skype is always doing its best to protect you from any kind of fraud. Sometimes this can cause perfectly legitimate purchases to be refused.

Learn about subscriptions

If you call phones regularly, you'll get the best rates with a subscription. Pay monthly for minutes to a destination of your choice.

Skype collects your IP upon payment - 07.03.2014, 11:23



A problem occurred while trying to access this page

We apologize for any inconvenience this might have

Reference number: #18.77c93451.1421934010.2af

HTTP status code: 403

European Central Bank
https://www.ecb.europa.eu
Search
ECB: European Central Ban...
File Edit View Favorites Tools Help
Convert Select
Herzogstand - Fahrenberg...
Page Safety Tools
EUROPEAN CENTRAL BANK
EUROSYSTEM
The European Central Bank | Press | Events | Publications | Statistics | The €uro | Monetary Policy | Payments & Markets
Direct access
Educational
Job opportunities
for suppliers
Economic research
Legal framework
Statistical Data Warehouse
Banking supervision
Key figures at a glance
Marginal lending facility 0.30 %
Main refinancing operations (fixed rate) 0.05 %
Deposit facility 0.20 %
Webcast of ECB press conference on 22 January 2015
Future events
Weekly schedule
Schedules for the meetings of the Governing Council
Eurosystem
ECB, ESCB and the Eurosystem
Educational games
€CONOMIA
Languages available
https://www.ecb.europa.eu/home/html/lingua.en.html
100%

Internet Explorer

TOR browser

22.1.2015, 14:42

7.7 Summary

- Patterns are helpful when implementing architectural goals.
- They provide proven solutions to requirements.
- There are dark patterns, too!