

Towards Privacy Management

Master Presentation for
Vidar Drageide

Department of Informathics
University of Bergen



UNIVERSITETET I BERGEN



Outline



Outline

- Defining privacy

Outline

- Defining privacy
- Privacy management

Outline

- Defining privacy
- Privacy management
- Sample privacy evaluation

Outline

- Defining privacy
- Privacy management
- Sample privacy evaluation
- Summary



Privacy

Privacy

- What is privacy?

Privacy

- What is privacy?
- A few definitions

Privacy

- What is privacy?
- A few definitions
- Do we really need it?

What is Privacy?

What is Privacy?

- «Everyone» knows what privacy is, but few can come up with a good definition

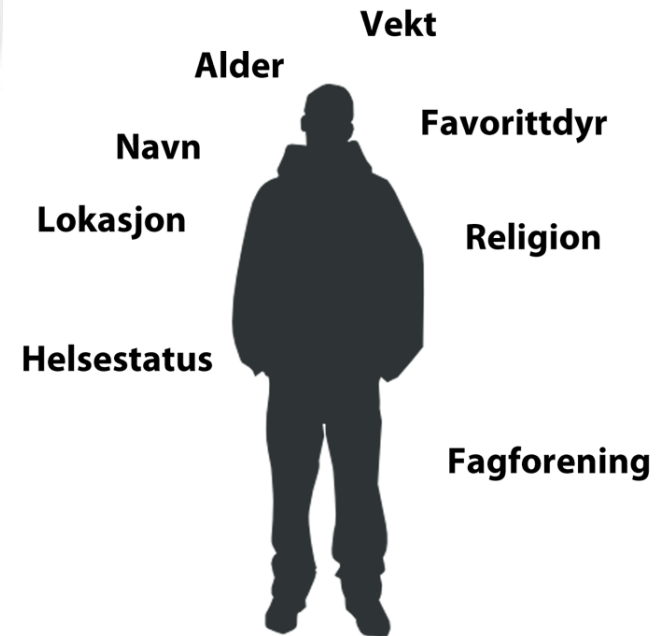
What is Privacy?

- «Everyone» knows what privacy is, but few can come up with a good definition
- A human right

What is Privacy?

- «Everyone» knows what privacy is, but few can come up with a good definition
- A human right
- Privacy in information systems

Two Important Definitions

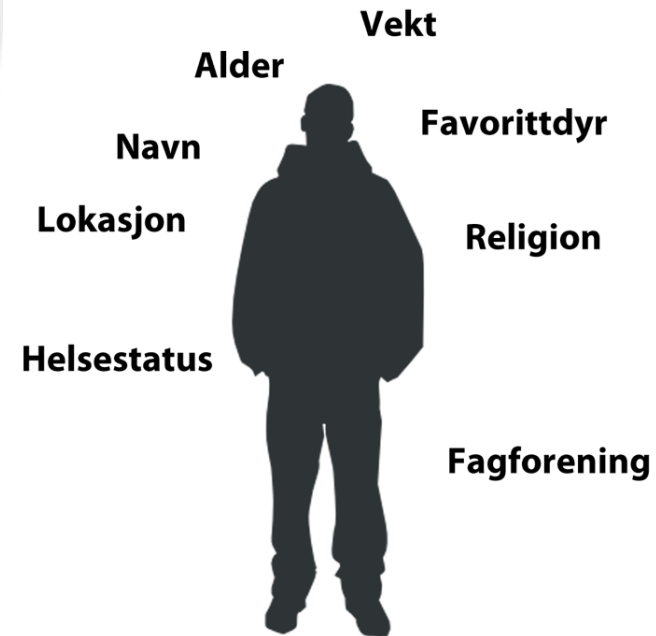


Two Important Definitions

- **Personal Information** – Information about an individual

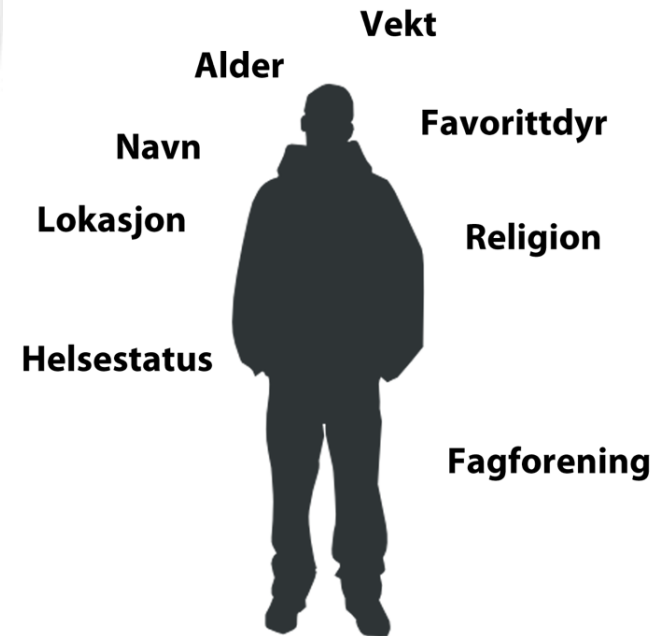
Two Important Definitions

- **Personal Information** – Information about an individual



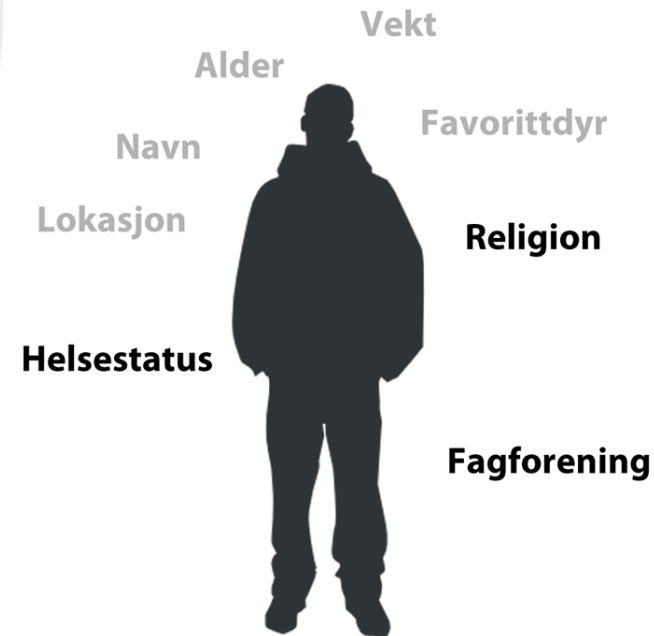
Two Important Definitions

- **Personal Information** – Information about an individual
- **Sensitive Personal Information** – Information about an individual that has a sensitive nature



Two Important Definitions

- **Personal Information** – Information about an individual
- **Sensitive Personal Information** – Information about an individual that has a sensitive nature





Do We Really Need Privacy?

Do We Really Need Privacy?

- At least in systems maintaining sensitive personal information

Do We Really Need Privacy?

- At least in systems maintaining sensitive personal information
- Privacy is a human right, and included in numerous laws and regulations

Do We Really Need Privacy?

- At least in systems maintaining sensitive personal information
- Privacy is a human right, and included in numerous laws and regulations
- Privacy is considered a requirement for democracy

My View on Privacy

Anonymity

Unlinkability

Untraceability

Personal Information

Collection

Retention

Secondary Use

Distribution

Distortion

Correction

Notification

My View on Privacy

- By looking at how privacy continues to fail, problem areas were detected

My View on Privacy

- By looking at how privacy continues to fail, problem areas were detected
- Nine Controls

My View on Privacy

- By looking at how privacy continues to fail, problem areas were detected
- Nine Controls
- Based on these, a method for analysing the privacy in a system was created

My View on Privacy

- By looking at how privacy continues to fail, problem areas were detected
- Nine Controls
- Based on these, a method for analysing the privacy in a system was created
- Not all are applicable for all systems

My View on Privacy

- By looking at how privacy continues to fail, problem areas were detected
- Nine Controls
- Based on these, a method for analysing the privacy in a system was created
- Not all are applicable for all systems

Anonymity

Unlinkability

Untraceability

Personal Information

Collection

Retention

Secondary Use

Distribution

Distortion

Correction

Notification

My View on Privacy

- By looking at how privacy continues to fail, problem areas were detected
- Nine Controls
- Based on these, a method for analysing the privacy in a system was created
- Not all are applicable for all systems
 - Online Bank

Anonymity

Unlinkability

Untraceability

Personal Information

Collection

Retention

Secondary Use

Distribution

Distortion

Correction

Notification

My View on Privacy

- By looking at how privacy continues to fail, problem areas were detected
- Nine Controls
- Based on these, a method for analysing the privacy in a system was created
- Not all are applicable for all systems
 - Online Bank

Anonymity

Unlinkability

Untraceability

Personal Information

Collection

Retention

Secondary Use

Distribution

Distortion

Correction

Notification

My View on Privacy

- By looking at how privacy continues to fail, problem areas were detected
- Nine Controls
- Based on these, a method for analysing the privacy in a system was created
- Not all are applicable for all systems
 - Online Bank
 - «Ask Dr. Online»

Anonymity

Unlinkability

Untraceability

Personal Information

Collection

Retention

Secondary Use

Distribution

Distortion

Correction

Notification

My View on Privacy

- By looking at how privacy continues to fail, problem areas were detected
- Nine Controls
- Based on these, a method for analysing the privacy in a system was created
- Not all are applicable for all systems
 - Online Bank
 - «Ask Dr. Online»

Anonymity

Unlinkability

Untraceability

Personal Information

Collection

Retention

Secondary Use

Distribution

Distortion

Correction

Notification

Controls



Controls

Anonymity

Controls

Anonymity	
Untraceability	It should no be possible to trace actions back to a user

Controls

Anonymity	
Untraceability	It should no be possible to trace actions back to a user
Unlinkability	It should not be possible to link actions performed by a specific user

Controls

Anonymity	
Untraceability	It should no be possible to trace actions back to a user
Unlinkability	It should not be possible to link actions performed by a specific user
Personal Information	

Controls

Anonymity	
Untraceability	It should no be possible to trace actions back to a user
Unlinkability	It should not be possible to link actions performed by a specific user
Personal Information	
Collection	Any information system should only collect the minimum amount of personal information that it needs to fulfil its purpose.

Controls

Anonymity	
Untraceability	It should no be possible to trace actions back to a user
Unlinkability	It should not be possible to link actions performed by a specific user
Personal Information	
Collection	Any information system should only collect the minimum amount of personal information that it needs to fulfil its purpose.
Retention	Personal information should be retained for the shortest possible period

Controls

Anonymity	
Untraceability	It should no be possible to trace actions back to a user
Unlinkability	It should not be possible to link actions performed by a specific user
Personal Information	
Collection	Any information system should only collect the minimum amount of personal information that it needs to fulfil its purpose.
Retention	Personal information should be retained for the shortest possible period
Secondary Use	Collected personal information should only be used for the specific purpose it was originally collected

Controls

Anonymity	
Untraceability	It should no be possible to trace actions back to a user
Unlinkability	It should not be possible to link actions performed by a specific user
Personal Information	
Collection	Any information system should only collect the minimum amount of personal information that it needs to fulfil its purpose.
Retention	Personal information should be retained for the shortest possible period
Secondary Use	Collected personal information should only be used for the specific purpose it was originally collected
Distribution	The personal information collected by any system should not be made available to third parties without prior consent from the data subject

Controls

Anonymity	
Untraceability	It should no be possible to trace actions back to a user
Unlinkability	It should not be possible to link actions performed by a specific user
Personal Information	
Collection	Any information system should only collect the minimum amount of personal information that it needs to fulfil its purpose.
Retention	Personal information should be retained for the shortest possible period
Secondary Use	Collected personal information should only be used for the specific purpose it was originally collected
Distribution	The personal information collected by any system should not be made available to third parties without prior consent from the data subject
Distortion	Operators of a system should do their best to assure the integrity of the information system

Controls

Anonymity	
Untraceability	It should no be possible to trace actions back to a user
Unlinkability	It should not be possible to link actions performed by a specific user
Personal Information	
Collection	Any information system should only collect the minimum amount of personal information that it needs to fulfil its purpose.
Retention	Personal information should be retained for the shortest possible period
Secondary Use	Collected personal information should only be used for the specific purpose it was originally collected
Distribution	The personal information collected by any system should not be made available to third parties without prior consent from the data subject
Distortion	Operators of a system should do their best to assure the integrity of the information system
Correction	Any individual whom the system stores personal information about should be able to access and correct data concerning self

Controls

Anonymity	
Untraceability	It should no be possible to trace actions back to a user
Unlinkability	It should not be possible to link actions performed by a specific user
Personal Information	
Collection	Any information system should only collect the minimum amount of personal information that it needs to fulfil its purpose.
Retention	Personal information should be retained for the shortest possible period
Secondary Use	Collected personal information should only be used for the specific purpose it was originally collected
Distribution	The personal information collected by any system should not be made available to third parties without prior consent from the data subject
Distortion	Operators of a system should do their best to assure the integrity of the information system
Correction	Any individual whom the system stores personal information about should be able to access and correct data concerning self
Notification	In the case of a mishap the users whose personal information was leaked and, perhaps, misused should be informed of the incident



Managing Privacy in Information Systems

Managing Privacy in Information Systems

- Use a structured approach

Managing Privacy in Information Systems

- Use a structured approach
- Start by getting a good overview of the system, what information it contains, and how it flows around

Managing Privacy in Information Systems

- Use a structured approach
- Start by getting a good overview of the system, what information it contains, and how it flows around
- Evaluate each control and rate it

Managing Privacy in Information Systems

- Use a structured approach
- Start by getting a good overview of the system, what information it contains, and how it flows around
- Evaluate each control and rate it
- Document the process, and make the documentation publicly available

Managing Privacy in Information Systems

- Use a structured approach
- Start by getting a good overview of the system, what information it contains, and how it flows around
- Evaluate each control and rate it
- Document the process, and make the documentation publicly available
- Create a short summary

Rating the Controls

Rating the Controls

- Qualitative rating

Rating the Controls

- Qualitative rating
- I have used High, Medium and Low

Rating the Controls

- Qualitative rating
- I have used High, Medium and Low

High - Control is Perfect

Medium - Good privacy, could be better

Low - Privacy is suffering

Sample Evaluation

- In my thesis I have carried out an evaluation of personal information in the cellphone system
- The evaluation was done without help from telcos



Collection

Collection

- Call Detail Records contain:
 - Number placing the call
 - Number receiving the call
 - Date and time
 - Duration (seconds)
 - Type of call (Voice, Data, SMS, ...)
 - The position of the parties (Base station and cell)

Collection

- Call Detail Records contain:
 - Number placing the call
 - Number receiving the call
 - Date and time
 - Duration (seconds)
 - Type of call (Voice, Data, SMS, ...)
 - The position of the parties (Base station and cell)
- Most of this is needed for billing, but not the parties position.

Distribution

Distribution

- Traffic data can be handed over to the police without a court ruling.

Distribution

- Traffic data can be handed over to the police without a court ruling.
- Network operators make APIs for geolocalization available through business to business solutions

Distribution

- Traffic data can be handed over to the police without a court ruling.
- Network operators make APIs for geolocalization available through business to business solutions
- As a result also this control is rated as medium

Summary of Evaluation

Collection	Retention	SecondaryUse	Distribution	Distortion
High	High	High	High	High
Medium	Medium	Medium	Medium	Medium
Low	Low	Low	Low	Low

Correction	Notification	Unlinkability	Untraceability
High	Missing	Not Applicable	Not Applicable
Medium			
Low			

Conclusions

Conclusions

- Privacy is important

Conclusions

- Privacy is important
- Many examples available on how systems fail

Conclusions

- Privacy is important
- Many examples available on how systems fail
- The structured approach suggested can contribute to detect areas where privacy is suffering

Conclusions

- Privacy is important
- Many examples available on how systems fail
- The structured approach suggested can contribute to detect areas where privacy is suffering
- Applying the method on the telephone system identified problem areas and uncovered potentially illegal conduct from telephone providers.

Further Work

Further Work

- Method
 - Refinements
 - Universal High,Medium,Low definitions?

Further Work

- Method
 - Refinements
 - Universal High,Medium,Low definitions?
- Applying the method on more systems
 - Applying the method on multiple large and different systems

Further Work

- Method
 - Refinements
 - Universal High,Medium,Low definitions?
- Applying the method on more systems
 - Applying the method on multiple large and different systems
- Traffic Data
 - Visualising the potential of such data
 - Vendor by vendor review

More Information

The thesis can be downloaded at:

<http://www.NoWires.org>

<http://www.bora.uib.no>