

Bachelor Thesis | State of the Art in linking privacy requirements to technical solutions

Nora Miftah El Kheir, 11.03.19, Garching

Chair of Software Engineering for Business Information Systems (sebis)
Faculty of Informatics
Technische Universität München
www.matthes.in.tum.de

1. Motivation

2. Research Questions and Approach

3. Privacy Frameworks

4. Comparison of the frameworks

5. Conclusion

"the right to be left alone"[1]

"the right to determine when, how and to what extend information about them is communicated to others"[2]



On the 25.05.18 the
General Data
Protection Regulation
(GDPR) came into
effect

It regulates the data
protection and privacy
for all companies
operating in the
European Union

Non-compliance could
result in high fines [3]

Challenges: the regulation is formulated as an open norm and doesn't consist of concrete suggestions how to implement the legal requirements

Goal: identification of frameworks which close the gap between privacy requirements and concrete technical solutions

1. Motivation

2. Research Questions and Approach

3. Privacy Frameworks

4. Comparison of the frameworks

5. Conclusion



RQ1: What is the state of the art in linking privacy requirements to technical solutions?



RQ2: What similarities and differences exist between the privacy frameworks?



RQ3: Which stages of the software development lifecycle are supported by the frameworks?

Approach: Literature review

- Based on Kitchenham [4]



Planning the review

1. Identification of the need for a review
2. Development of a review protocol.



Conducting the review

1. Identification of research
2. Selection of primary studies
3. Study quality assessment
4. Data extraction & monitoring
5. Data synthesis.



Reporting the review

Used databases: Scopus, IEEE Xplore

Search term:

(((privacy AND requirement) AND (technical AND solutions OR technical AND implementation)) OR linking AND privacy AND requirements AND to AND implementations OR ((gdpr) AND (implementation OR methods)) OR (data AND protection AND implementation AND laws))

Results:

Step	Search with searchterm	Filter	Delete duplicates	Titles	Abstracts	Access	Back- & Forward search	Keypaper
Papers	330	223	215	25	14	12	14	13

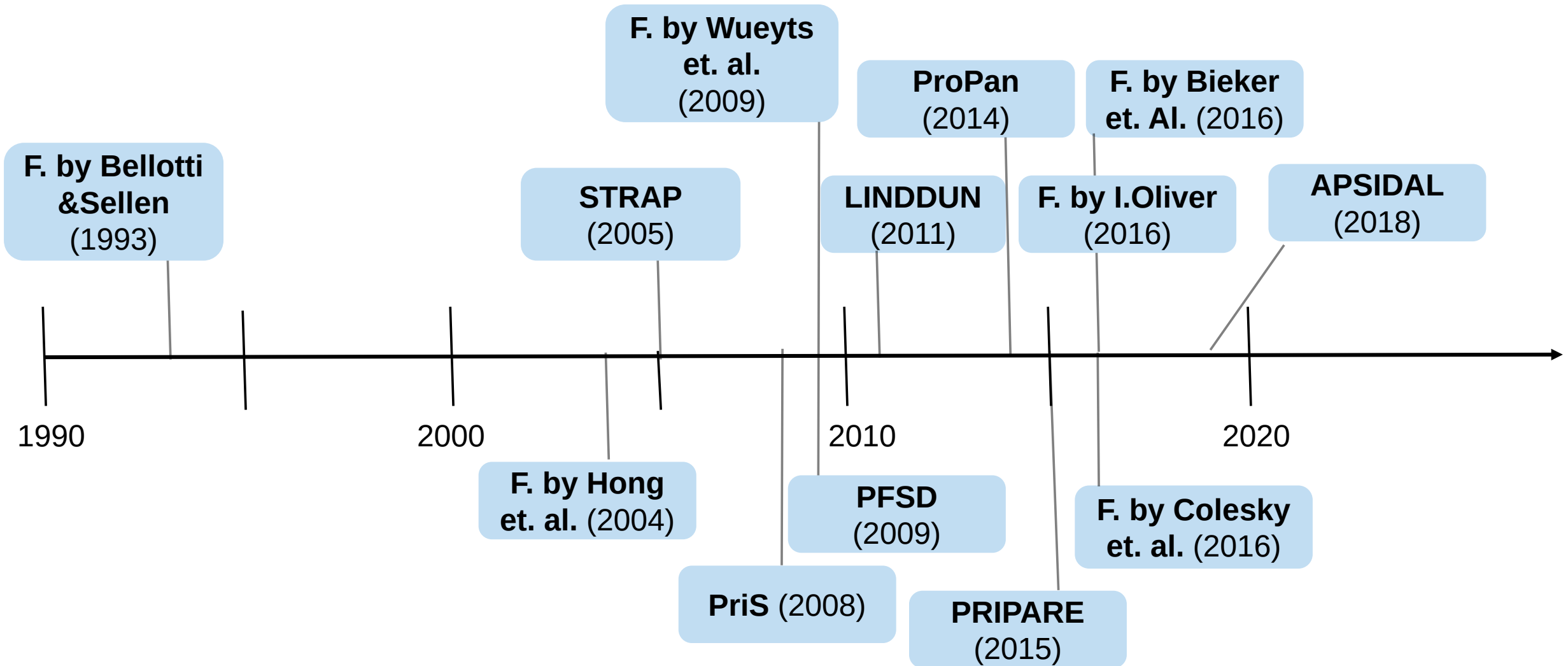
1. Motivation

2. Research Questions and Approach

3. Privacy Frameworks

4. Comparison of the frameworks

5. Conclusion



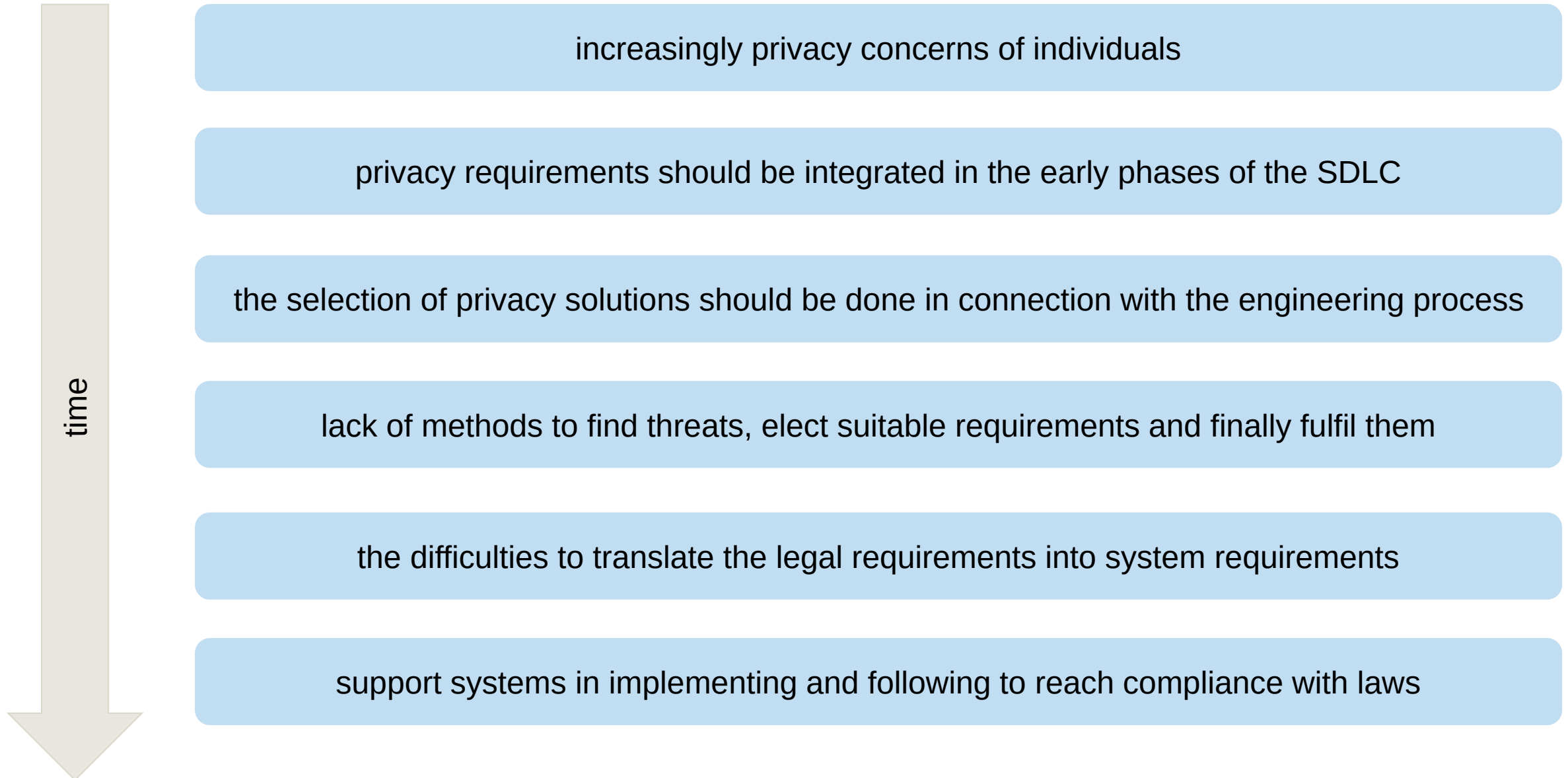
1. Motivation

2. Research Questions and Approach

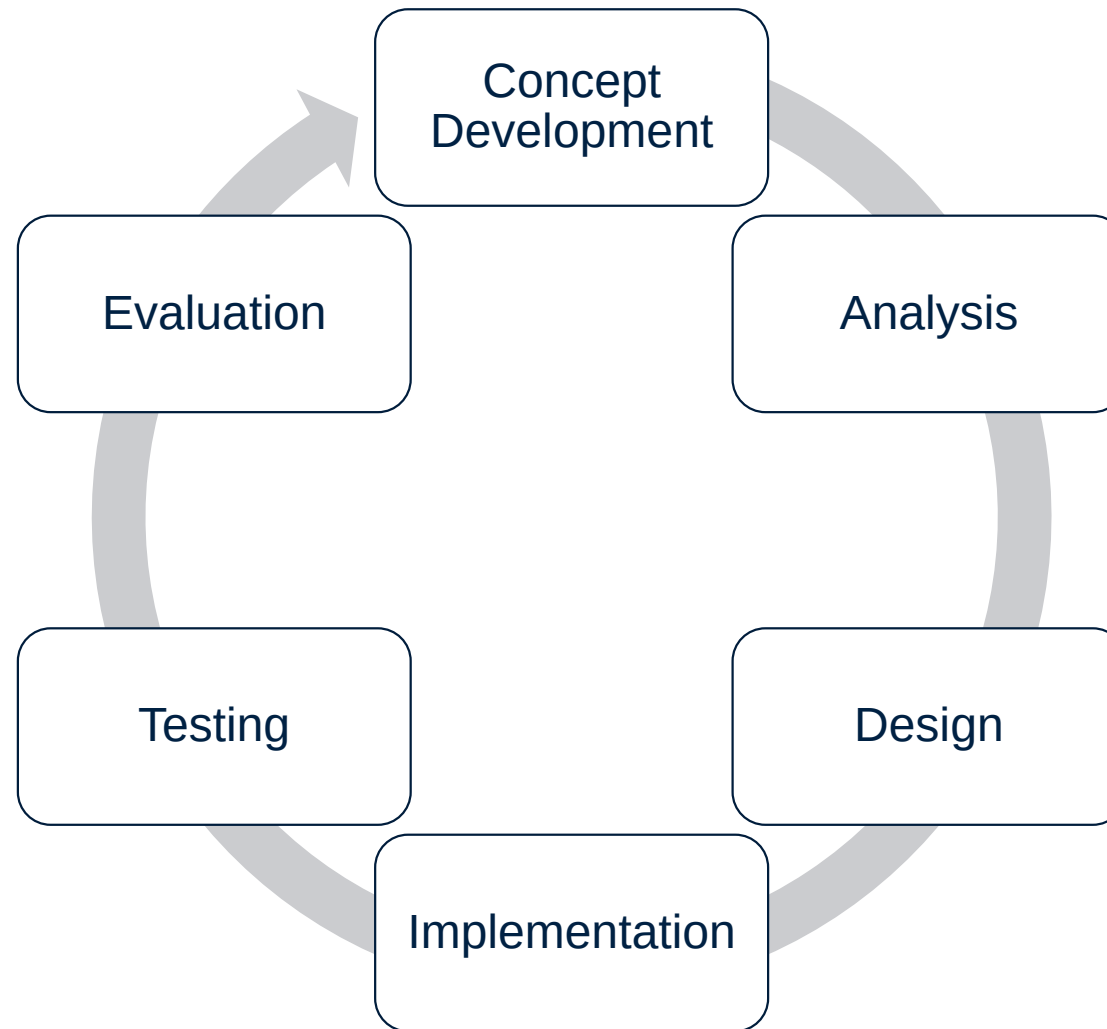
3. Privacy Frameworks

4. Comparison of the frameworks

5. Conclusion



Software Development Lifecycle



[6]

	CD	A	D	I	T	E
Framework by Bellotti and Sellen		X	X			
Framework by Hong et. al.		X	X			
STRAP		X	X			
PRIS	X	X	X	X		
Framework by Wuyts et. al.		X	X	X		
PFSD	X	X	X	X		
LINDDUN	X	X	X	X		
ProPan		X	X			
PRIPARE	X	X	X	X	X	X
Framework by Nokia		X	X			
Bieker et. al.	X	X	X	X	X	X
Colesky et. al.	X	X	X			
APSIDAL	X	X	X	X		

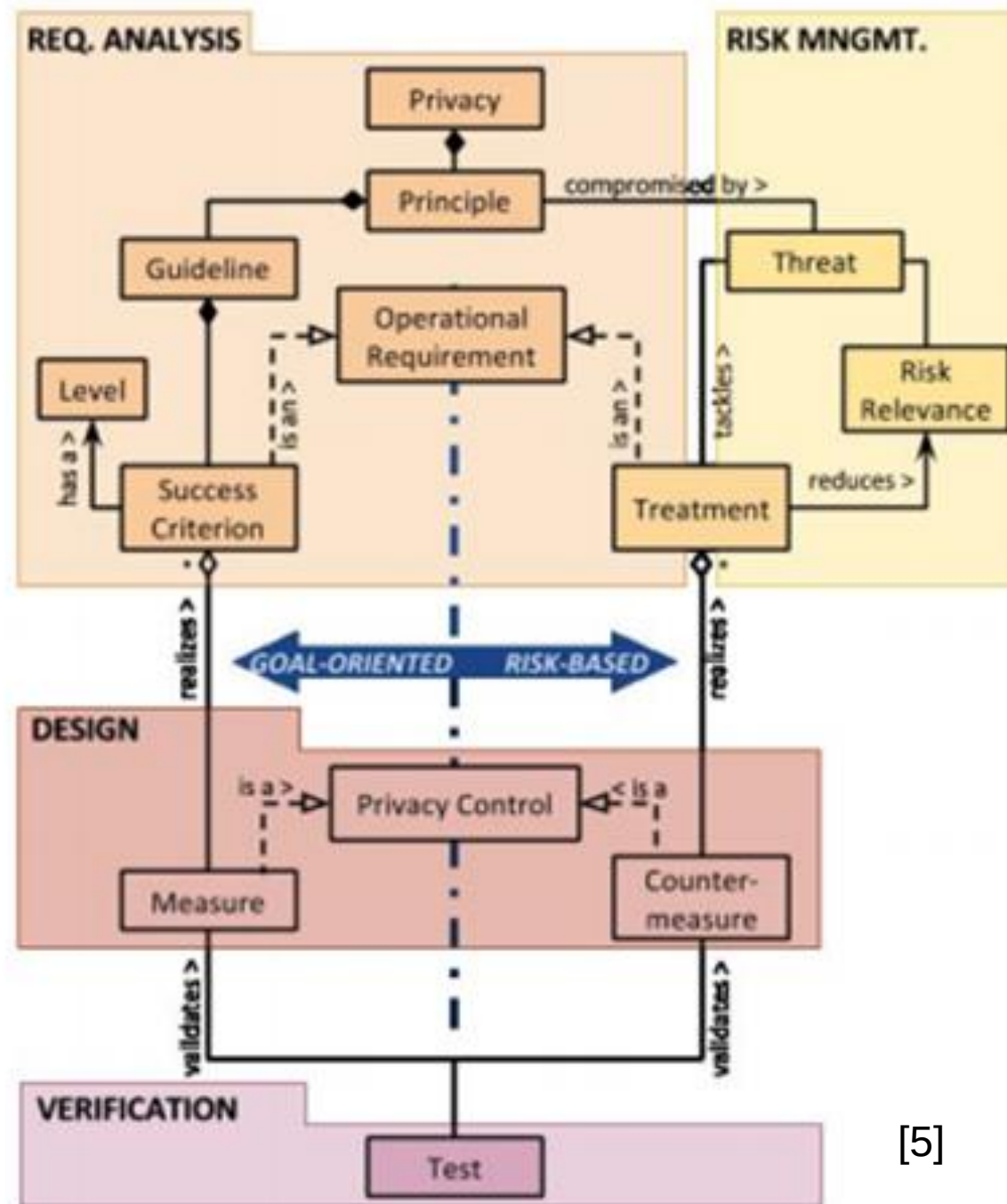
Origin of the privacy principles

	FIPS	Laws (GDPR)	Security properties	Research	No information
Framework by Bellotti and Sellen					X
STRAP	X				
PRIS			X	X	
PFSD	X				
LINDDUN				X	X
Framework by Bieker et. al.		X	X	X	
APSIDAL		X			

Privacy principles

	Framework by Bellotti and Sellen	STRAP	PRIS	PFSD	LINDDUN	Framework by Bieker et. al.	APSIDAL
Anonymity			X		X		
Pseudonymity			X		X		
Unlinkability			X		X	X	
Undetectability & Unobservability			X		X		
Transparency						X	X
User Content awareness	X	X		X	X		
Policy and Consent Compliance	X	X		X		X	X
Purpose Limitation						X	X
Data Minimization						X	X
Security Properties		X	X	X	X	X	X

Risk-based or Goal-oriented



[5]

Risk-based or Goal-oriented

	Risk-based	Goal-oriented
Framework by Bellotti and Sellen	X	
Framework by Hong et. al.	X	
STRAP		X
PRIS		X
Framework by Wuyts et. al.		X
PFSD	X	X
LINDDUN	X	
ProPan	X	
PRIPARE	X	X
Framework by Nokia		
Bieker et. al.	X	
Colesky et. al.		
APSIDAL	X	X

Six frameworks provide concrete technical solutions
(Privacy Enhancing Technologies)

Similarities:

- Provide concrete PETs
- Partly the same categories to classify the solutions

Differences:

- In the development approach:
based on the privacy principles
or based on the PETs
- The fineness of the distinction
- Number of the provided PETs

1. Motivation

2. Research Questions and Approach

3. Privacy Frameworks

4. Comparison of the frameworks

5. Conclusion



Different conceptual possibilities exist to build a privacy framework:

- covered stages of the SDLC
- underlying privacy principles
- approach to identify the operational privacy requirement
- distribution of the provided solutions



- 1) To what extent are the frameworks applied in practices?
- 2) How must the frameworks be changed that they can be used in agile software development processes?

- [1] Christos Kalloniatis and Evangelia Kavakli and Stefanos Gritzalis. 2007. Using Privacy Process Patterns for Incorporating Privacy Requirements into the System Design Process
- [2] Christos Kalloniatis and Evangelia Kavakli and Stefanos Gritzalis. 2008. Addressing privacy requirements in system design: the PriS method
- [3] Trunomi. The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years. URL: <https://eugdpr.org/>, accessed January 15, 2019
- [4] Barbara Kitchenham. 2004. Procedures for Performing Systematic Reviews
- [5] Nicolás Notario, Alberto Crespo, Yod-Samuel Martín, Jose M. del Alamo, Daniel Le Métayer, Thibaud Antignac, Antonio Kung, Inga Kroener, David Wright. 2015. PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology
- [6] Jaap-Henk Hoepman. 2013. Privacy Design Strategies



Nora Miftah El Kheir

Technische Universität München
Faculty of Informatics
Chair of Software Engineering for Business
Information Systems

Boltzmannstraße 3
85748 Garching bei München

Tel +49.89.289.
Fax +49.89.289.17136

nora.miftah@web.de
www.matthes.in.tum.de

