Subjectivity and Automation in Privacy Risk Assessment

Mario Raciti

Hardening Seven

IMT SCHOOL FOR ADVANCED STUDIES LUCCA

Università di Catania

27/03/23 – Catania

Agenda

1. **Intro to Privacy Risk Assessment**
2. **Intro to Privacy Threat Modelling**
3. **Embracing Approach**
4. **Combinatoric Approach**
5. **AILA Methodology**
6. **Conclusions**

Agenda

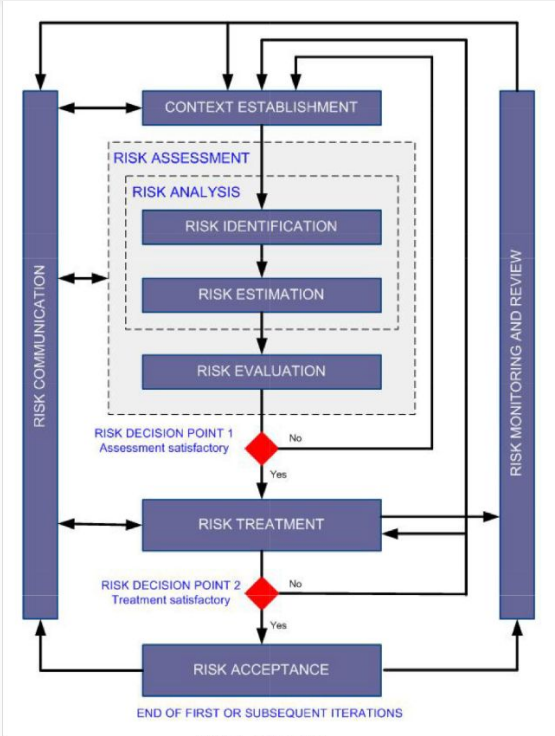
1. **Intro to Privacy Risk Assessment**
2. Intro to Privacy Threat Modelling
3. Embracing Approach
4. Combinatoric Approach
5. AILA Methodology
6. Conclusions

Privacy may be summarised as “the right of the data subject to control or influence what information related to them may be collected, processed and stored, and by whom and to whom that information may be disclosed.”

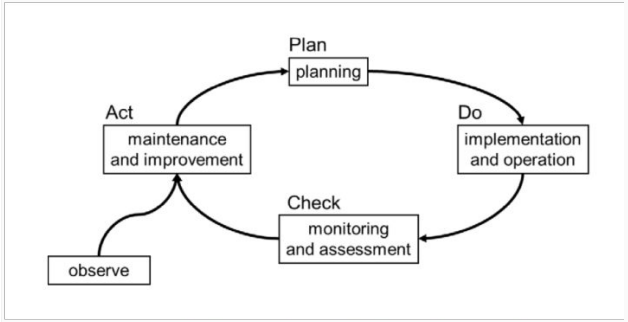
- GDPR Interpretation

Intro to (Privacy) Risk Assessment

"If you don't invest in risk management, it doesn't matter what business you're in, it's a risky business." - Gary Cohn



ISO 27005



ISMS PDCA Cycle [ISO 27001]

Risk Assessment in a Nutshell

RA inputs:

- Assets
- Threats
- Safeguards

RA outputs:

- Impact
- Risk

Risk		Likelihood				
		VL	L	M	H	VH
Impact	VH	H	VH	VH	VH	VH
	H	M	H	H	VH	VH
	M	L	M	M	H	H
	L	VL	L	L	M	M
	VL	VL	VL	VL	L	L

Other factors:

- Security dimensions
- Likelihood

Risk for dummies $R = L \times I$

Actual risk $R = \ldots ?$

where R is the risk, L the likelihood and I the impact.

Privacy Risk Assessment is “a process that helps organisations to analyse and assess privacy risks for individuals arising from the processing of their data.”

- NIST

Agenda

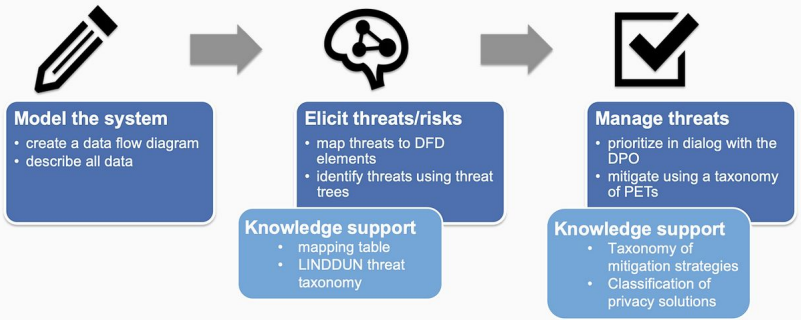
1. Intro to Privacy Risk Assessment
2. **Intro to Privacy Threat Modelling**
3. Embracing Approach
4. Combinatoric Approach
5. AILA Methodology
6. Conclusions

“**Threat modelling** works to identify, communicate, and understand threats and mitigations within the context of protecting something of value.”

- OWASP

Privacy Threat Modelling with LINDDUN

LINDDUN is a privacy threat modelling methodology that supports analysts in systematically eliciting and mitigating privacy threats in software architectures.



Linkability
An adversary is able to link two items of interest without knowing the identity of the data subject(s) involved.

Identifiability
An adversary is able to identify a data subject from a set of data subjects through an item of interest.

Non-repudiation
The data subject is unable to deny a claim (e.g., having performed an action, or sent a request).

Detectability
An adversary is able to distinguish whether an item of interest about a data subject exists or not, regardless of being able to read the contents itself.

Disclosure of information
An adversary is able to learn the content of an item of interest about a data subject.

Unawareness
The data subject is unaware of the collection, processing, storage, or sharing activities (and corresponding purposes) of the data subject's personal data.

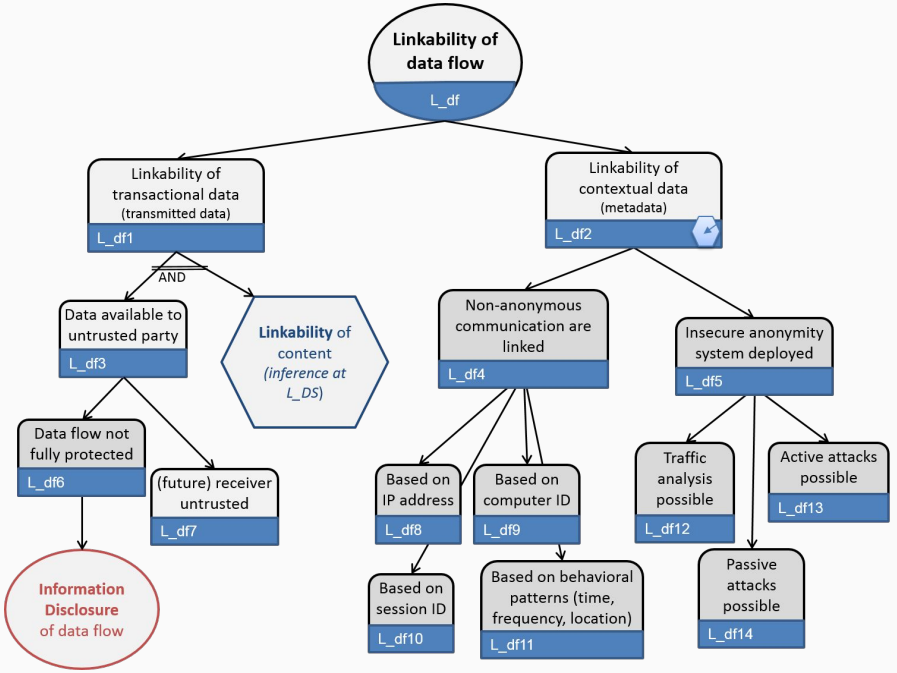
Non-compliance
The processing, storage, or handling of personal data is not compliant with legislation, regulation, and/or policy.

LINDDUN Knowledge Base

LINDDUN provides a set of threats specific to privacy, named as “threat catalogue”, in the form of threat trees.

The root node represents the ultimate goal.

The children nodes embody different ways of achieving that goal.



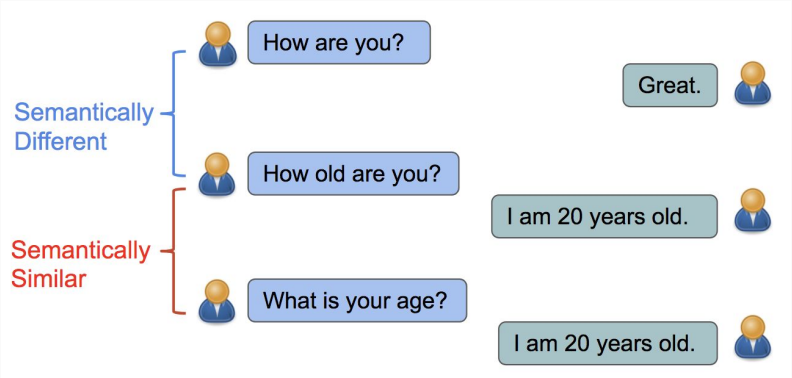
How to Model Privacy Threats for a Privacy RA?

Agenda

1. Intro to Privacy Risk Assessment
2. Intro to Privacy Threat Modelling
3. **Embracing Approach**
4. Combinatoric Approach
5. AILA Methodology
6. Conclusions

Embracing Approach

Threat embracing wants to capture the **standard scrutiny** that the analyst operates in front of a list of threats to understand the extent of their **semantic similarity**.



Embracing Approach

Elements of scrutiny derive from:

- the use of **synonyms** (e.g., “protocol” and “distributed algorithm”).
- the **level of detail** (e.g., “Unchanged default password” and “Human error”).

The analyst would conclude whether these threats are embraceable and embrace them by selecting the one with the wording/level of detail that they find most appropriate, and discarding the other one.

A Systematic Method

Step 1 — Threat Collection: involves the collection of the threats that the analyst deems relevant.

Step 2 — Categorisation: categorises each preliminary threat with respect to the LINDDUN properties.

Step 3 — Manipulation: defines a list of operations to build the final threats upon the basis of the preliminary threats.

Step 4 — Mapping: consists in verifying whether the LINDDUN threat catalogue covers the final threats and vice versa.

Step 5 — Safety Check: implements a further safety check of Step 2, when we may have assigned an insufficient list of pertaining properties to the preliminary threats that were later embraced in some final threat.

Agenda

1. Intro to Privacy Risk Assessment
2. Intro to Privacy Threat Modelling
3. **Embracing Approach → Automotive Demo**
4. Combinatoric Approach
5. AILA Methodology
6. Conclusions

Automotive Demo - Step 1

P	LB	S
p_13	Abuse of authorizations	ENISA
p_14	Sabotage	ENISA
p_15	Theft	ENISA
p_16	Side-channel attacks	ENISA
p_17	Fault injection	ENISA
p_18	Software vulnerabilities exploitation	ENISA
p_19	Failure or Disruption of service	ENISA
p_20	Communication protocol hijacking	ENISA
p_21	Data replay	ENISA
p_22	Man-in-the-middle attack / Session hijacking	ENISA
p_23	Unintentional change of data or car components configuration	ENISA
p_24	Information leakage	ENISA
p_25	Using information and/or devices from an unreliable source	ENISA
p_26	Erroneous use or configuration of car components	ENISA
p_27	Failure to meet contractual requirements	ENISA
p_28	Violation of rules and regulations/Breach of legislation/ Abuse of	ENISA
p_29	Loss of GNSS signal	ENISA
p_30	Car depleted battery	ENISA
p_31	Attacker injects CAN messages/codes via any ECUs connected	Chah et al.
p_32	Attacker modifies the path of the sensitive data circulating in the	Chah et al.
p_33	Attacker remotely accesses via telematics systems (TCU).	Chah et al.
p_34	An adversary can capture, analyze, and replaye the messages.	Chah et al.
p_35	An adversary could link the messages to a specific vehicle	Chah et al

P	LB	S
p_45	Reprogramming the USB/CD device's firmware to execute malic	Chah et al
p_46	An adversary can exploit the vulnerabilities o USB svstems on-b	Chah et al
p_47	An adversary can identify or track the vehicle from the sensor.	Chah et al
p_48	For wireless communication channel, messages can be capture	Chah et al
p_49	Possibility to discover and control the behaviour and profile of th	Chah et al
p_50	An adversary relates pseudonymous positions to specific vehicle	Chah et al
p_51	Mobile App spoofing	Bella et al.
p_52	Smart key bruteforcing	Bella et al.
p_53	Smart key cloning	Bella et al.
p_54	GPS spoofing	Bella et al.
p_55	V2X Message replay	Bella et al.
p_56	Infotainment malware	Bella et al.
p_57	Mobile App malware	Bella et al.
p_58	ECU reflash	Bella et al.
p_59	CAN frame injection	Bella et al.
p_60	CAN frame tampering	Bella et al.
p_61	V2X data tampering	Bella et al

Automotive Demo - Step 2

P	LB	S	L	I	N	D	Di	U	Nc
p_1	Denial of Service	ENISA			✓	✓			
p_2	Malware	ENISA	✓	✓		✓	✓		
p_3	Manipulation of hardware and software	ENISA	✓	✓	✓	✓	✓		
p_4	Manipulation of information	ENISA	✓	✓	✓	✓	✓		
p_5	Threats targeting autonomous sensors	ENISA	✓	✓					
p_6	Threats against AI and ML	ENISA							
p_7	Failure or malfunction of a sensor/actuator	ENISA				✓			
p_8	Vandalism	ENISA							
p_9	Network outage	ENISA			✓				
p_10	OEM Targeted attacks	ENISA	✓				✓		
p_11	Unauthorised activities	ENISA					✓		
p_12	Identity theft	ENISA		✓			✓		
p_13	Abuse of authorizations	ENISA					✓		
p_14	Sabotage	ENISA			✓				
p_15	Theft	ENISA		✓			✓		
p_16	Side-channel attacks	ENISA					✓		
p_17	Fault injection	ENISA			✓				
p_18	Software vulnerabilities exploitation	ENISA	✓	✓	✓	✓	✓		
p_19	Failure or Disruption of service	ENISA			✓				
p_20	Communication protocol hijacking	ENISA	✓	✓		✓	✓		

Automotive Demo - Step 3

F	LB	S	L	I	N	D	Di	U	Nc
f_1	Abuse of authorisations *in OEM and/or car services*	rename(embrace(p_13, p_75))					✓		
f_2	CAN bus flooding	embrace(p_69, p_11)			✓				
f_3	CAN eavesdropping	p_62				✓	✓		
f_4	CAN frame injection	embrace(p_59, p_3, p_31)	✓	✓	✓	✓	✓		
f_5	CAN frame tampering	embrace(p_60, p_3, p_40, p_48)				✓			
f_6	Change of data or car components configuration	rename(embrace(p_23, p_41, p_42))	✓	✓	✓		✓		
f_7	Communication protocol hijacking *in car devices*	rename(embrace(p_20, p_32))	✓	✓	✓	✓	✓		
f_8	Data aggregation and profiling *of driver*	rename(embrace(p_39, p_49, p_50))	✓	✓			✓		
f_9	Data loss *in OEM and/or car services*	rename(embrace(p_71, p_1))			✓				
f_10	ECU firmware dump	p_66					✓		
f_11	ECU reflash	p_58		✓					
f_12	Erroneous use or configuration of car components	p_26	✓				✓		
f_13	Failure to meet contractual requirements *with driver*	rename(p_27)							✓
f_14	Failures or sabotage *of car components*	rename(embrace(p_7, p_9, p_14, p_19))			✓				
f_15	GPS spoofing	embrace(p_54, p_48)					✓		
f_16	Identity theft *of driver*	rename(p_12)			✓		✓		
f_17	Infotainment alteration	embrace(p_73, p_3, p_37, p_43, p_44)	✓	✓	✓		✓		
f_18	Infotainment malware	embrace(p_56, p_2)	✓	✓			✓		
f_19	Infotainment reverse engineering	embrace(p_64, p_3)					✓		
f_20	Loss of GNSS signal	p_29			✓				
f_21	Man-in-the-middle attack / Session hijacking *in OEM and/or car services*	rename(p_22)	✓	✓		✓	✓		
f_22	Manipulation of information *in OEM and/or car services*	rename(p_4)	✓	✓	✓	✓	✓		

Automotive Demo - Step 4

Linkability	Threat(s)	Identifiability	Threat(s)	Non-repudiation	Threat(s)	Detectability	Threat(s)	Disclosure of information	Threat(s)	Unawareness	Threat(s)	Non-compliance	Threat(s)
L_e		***I_e***		***NR_df***		***D_df***		***ID_df***		***U***		***NC***	
L_e1	f_17, f_18, f_23,	I_e1	f_23, f_24	NR_df1	f_6, f_14, f_17	D_df1	f_32	ID_df1	f_1	U_1	f_32	NC_1	f_41
L_e2		I_e2		NR_df2	f_7, f_14, f_32	D_df2	f_32, f_37, f_40	ID_df2	f_1, f_7, f_8	U_2	f_32	NC_2	
L_e3	f_7, f_36	I_e3	f_6, f_7, f_36	NR_df3	f_32	D_df3	f_32	ID_df3	f_18, f_19,	U_3		NC_3	
L_e4	f_40	I_e4		NR_df4	f_32	D_df4	f_32	ID_df4	f_3	U_4		NC_4	
L_e5	f_32	I_e5		NR_df5	f_2, f_7, f_20	D_df5	f_32	ID_df5		U_5	f_32		
L_e6	f_25, f_33	I_e6		NR_df6		D_df6		ID_df6	f_6, f_15, f_17, f_21, f_33				
L_df		I_e7		NR_df7	f_24	D_df7	f_5, f_7, f_21, f_	ID_df7					
L_df1		I_e8		NR_df8		D_df8		***ID_ds***					
L_df2		I_e9		NR_df9		D_df9	f_4, f_36, f_39	ID_ds1	f_10, f_16, f_29, f_33				
L_df3	f_25, f_33, f_36	I_e10		NR_df10	f_16, f_33, f_3	D_df10		ID_ds2	f_7, f_19				
L_df4	f_8	I_e11		NR_df11		D_df11		ID_ds3	f_7, f_8, f_15, f_18, f_23, f_25				
L_df5	f_6, f_12, f_17, f	I_e12		NR_df12	f_22	D_df12		ID_ds4	f_17, f_25, f_28				
L_df6	f_7, f_32, f_34, f	I_e13		NR_df13	f_41	D_df13		ID_ds5	f_1, f_6, f_8, f_10, f_17, f_22, f_35, f_36				
L_df7		I_e14	f_32	NR_df14		***D_ds***		ID_ds6	f_12				
L_df8		I_e15		NR_df15		D_ds1	f_32, f_35	ID_ds7	f_32				
L_df9		I_e16		NR_df16		D_ds2	f_32	ID_ds8	f_32, f_35				
L_df10		I_e17		NR_df17	f_22	D_ds3	f_7	ID_ds9					
L_df11		I_e18		NR_df18				ID_ds10	f_32				
L_df12	f_7, f_21, f_34	I_e19	f_33	***NR_ds***				ID_ds11	f_32				
L_df13	f_4, f_21, f_22, f	I_e20	f_32	NR_ds1	f_4, f_7			ID_ds12	f_32				

Automotive Demo - Step 5

s)	Unawareness	Threat(s)	Non-compliance	Threat(s)
	U		***NC***	
	U_1	f_32	NC_1	f_41
f_8	U_2	f_32	NC_2	
19,	U_3		NC_3	
	U_4		NC_4	
	U_5	f_32	NC_5	f_13
5, f_17, f_21, f_33			NC_6	f_41
16, f_29, f_33				

f_13 "Failure to meet contractual requirements"

f_41 "Violation of rules and regulations/Breach of legislation/Abuse of personal data"

Automotive Demo - Results

The full outcomes include 95 preliminary and **56 detailed final privacy threats**.

The application of our systematic method highlighted that there are final threats that are not embraceable with any LINDDUN node according to the analyst's judgement.

Table 7: Final threats from the automotive and web domains that we could not match to any LINDDUN threat.

F	LB	S
f_{13a}	Failure to meet contractual requirements	p_{27a}
f_{41a}	Violation of rules and regulations/Breach of legislation/ Abuse of personal data	p_{28a}
f_{2w}	Consent-related issues	$rename(embrace(p_{4w}, p_{17w}))$
f_{4w}	Inability of users to access and modify data	p_{9w}
f_{7w}	Insufficient Data Breach Response	p_{3w}
f_{11w}	Misleading Content	p_{16w}
f_{13w}	Secondary Use	p_{19w}
f_{14w}	Sharing, Transfer or Processing through 3rd Party	$rename(embrace(p_{12w}, p_{15w}))$

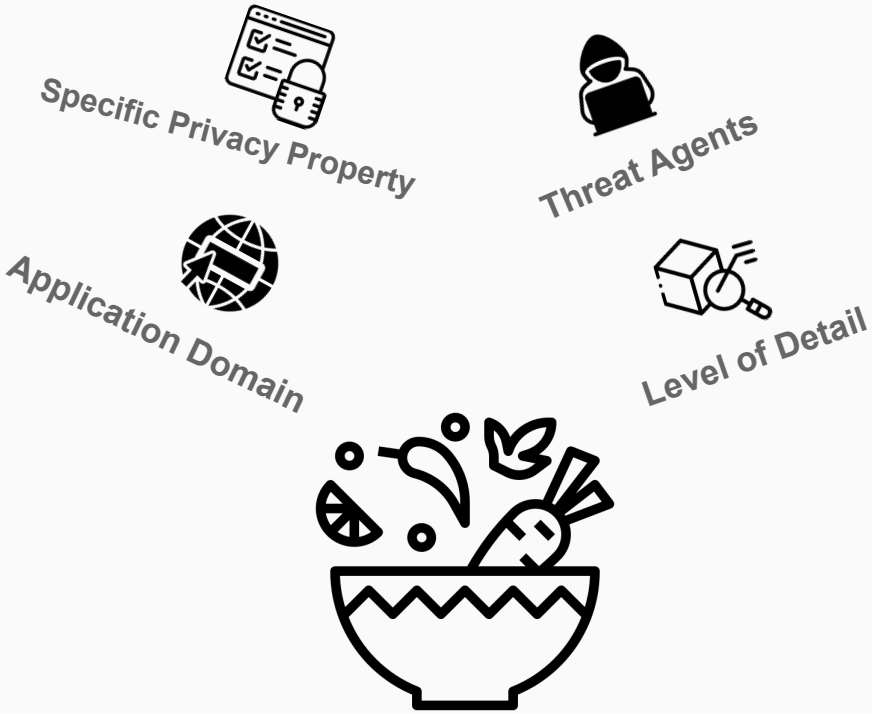
What is the main drawback of this approach?

...subjectivity!

Agenda

1. Intro to Privacy Risk Assessment
2. Intro to Privacy Threat Modelling
3. Embracing Approach
4. **Combinatoric Approach**
5. AILA Methodology
6. Conclusions

Privacy Threat Modelling Ingredients



Specific Privacy Property

> Hard Privacy
> Soft Privacy
> Cybersecurity

Cybersecurity plays a complementary role in terms of protection against the unauthorised access of data.

Threat Agents

> Attacker
> Data processor
> Data controller
> Third party

TAs may also be considered in combination.

Application Domain

> Domain-Dependent
> Domain-Independent

A combination of the two approaches may offer a more effective and efficient analysis.

Level of Detail

> Hyponym (higher / detailed)
> Hypernym (lower / abstract)

A hyponym implies a more precise likelihood estimation. However, an excessive level of detail leads to an exact assignment of the likelihood (either the bottom or the top value).

Combinatoric Approach

Step 1 — Domain-Independent Threat Elicitation: involves the collection of the threats that the analyst deems relevant.

Step 2 — Domain-Dependent Asset Collection: consists of the collection of a list of assets for the target domain from relevant sources.

Step 3 — Domain-Dependent Threat Elicitation: produces a list of domain-specific threats.

Agenda

1. Intro to Privacy Risk Assessment
2. Intro to Privacy Threat Modelling
3. Embracing Approach
4. **Combinatoric Approach → Automotive Demo**
5. AILA Methodology
6. Conclusions

Automotive Demo

Soft Privacy

Domain-dependent

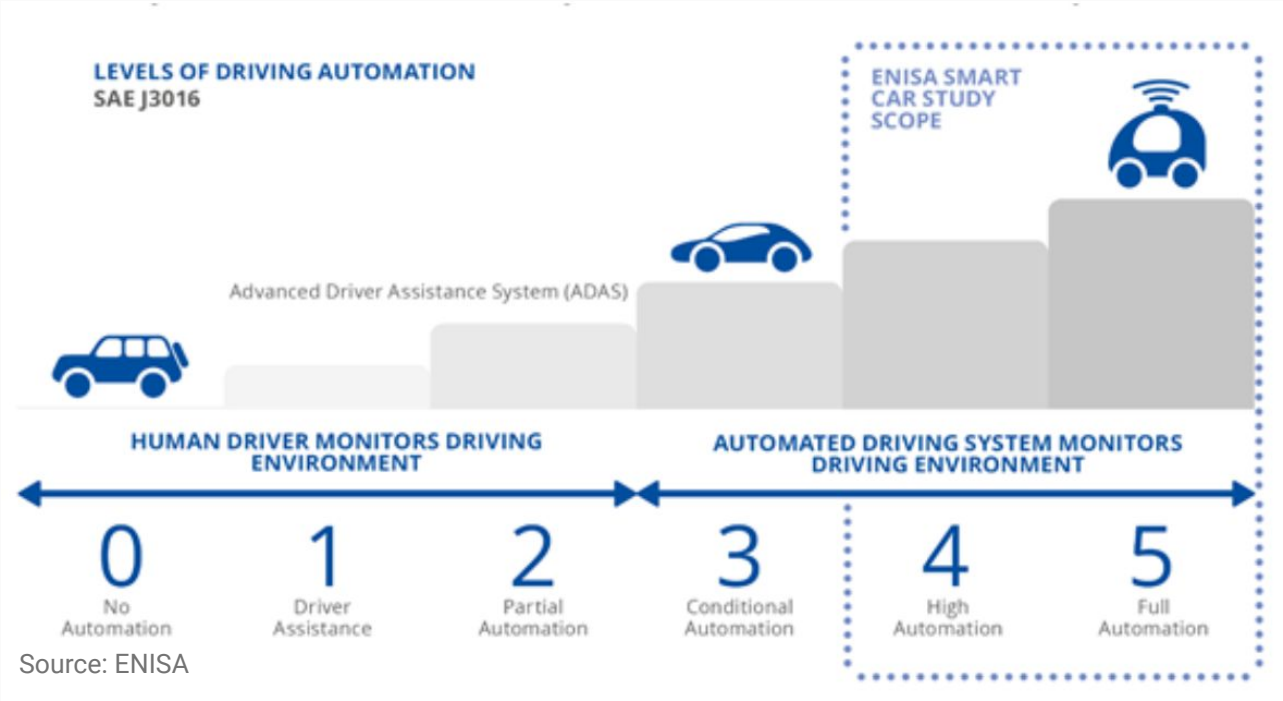
Attacker, Data processor/controller, Third party

Abstract (Hypernym)

Automotive Demo – Step 1

Source	Threat
U	Providing too much personal data
	Unaware of stored data
	No/insufficient feedback and awareness tools
	No user-friendly privacy support
	Unable to review personal information (data accuracy)
N	Attacker tampering with privacy policies and makes consents inconsistent
	Incorrect or insufficient privacy policies
	Inconsistent/insufficient policy management
	Insufficient notice
ENISA	Failure to meet contractual requirements
	Violation of rules and regulations/Breach of legislation/ Abuse of personal
OWASP	Consent-related issues
	Inability of user to access and modify data
	Insufficient data breach response
	Misleading content
	Secondary use
	Sharing, transfer or processing through 3rd party

Automotive Demo – Step 2



Source: ENISA

Automotive Demo – Step 3

TABLE 2. RESULTS OF THE APPLICATION OF OUR METHODOLOGY TO THE AUTOMOTIVE DOMAIN: LIST OF SOFT PRIVACY THREATS.

Source	Threat	Assets
U	Providing too much personal data	User information, Special categories of personal data
	Unaware of stored data	Map data, V2X information, Device information, User information, Special categories of personal data, User preferences, Purchase information
	No/insufficient feedback and awareness tools	Map data, Device information, User information, Special categories of personal data, Driver's behaviour, User preferences, Purchase information
	No user-friendly privacy support	Sensors data, Map data, V2X information, Device information, User information, Special categories of personal data, Driver's behaviour, User preferences, Purchase information
	Unable to review personal information (data accuracy)	User information, Special categories of personal data
N	Attacker tampering with privacy policies and makes consents inconsistent	Sensors data, Key and certificates, Map data, V2X information, Device information, User information, Special categories of personal data, Driver's behaviour, User preferences, Purchase information
	Incorrect or insufficient privacy policies	All assets
	Inconsistent/insufficient policy management	All assets
	Insufficient notice	Sensors data, Key and certificates, Map data, V2X information, Device information, User information, Special categories of personal data
ENISA	Failure to meet contractual requirements	All assets
	Violation of rules and regulations/Breach of legislation/ Abuse of personal data	All assets
OWASP	Consent-related issues	All assets
	Inability of user to access and modify data	Map data, V2X information, Device information, User information, Special categories of personal data, User preferences, Purchase information
	Insufficient data breach response	Sensors data, Key and certificates, Map data, V2X information, Device information, User information, Special categories of personal data, User preferences, Purchase information
	Misleading content	Map data, V2X information, Device information, User information, Special categories of personal data, User preferences
	Secondary use	All assets
	Sharing, transfer or processing through 3rd party	Sensors data, Key and certificates, Map data, V2X information, Device information, User information, Special categories of personal data, Driver's behaviour, User preferences, Purchase information

Automotive Demo – Results

The full outcomes include **17 soft privacy threats**.

These threats are both *domain-independent* and *domain-dependent*.

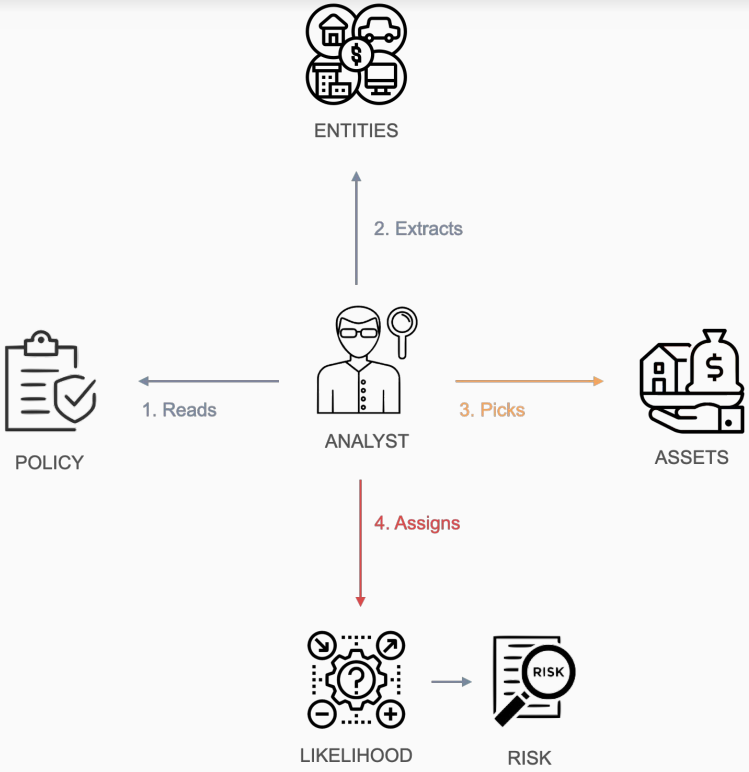
What is the main drawback of this approach?

…handwork!

Agenda

1. Intro to Privacy Risk Assessment
2. Intro to Privacy Threat Modelling
3. Embracing Approach
4. Combinatoric Approach
5. **AILA Methodology**
6. Conclusions

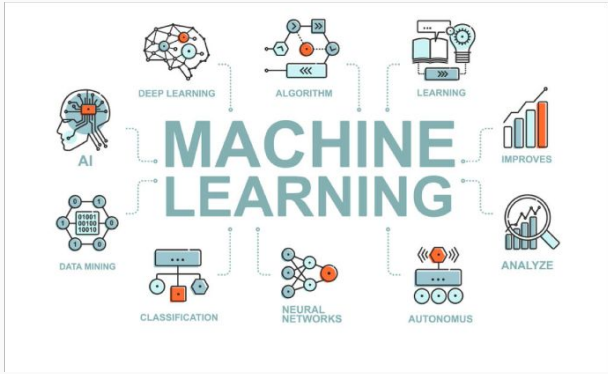
Privacy Policy RA



Automated and Intelligent Likelihood Assignment

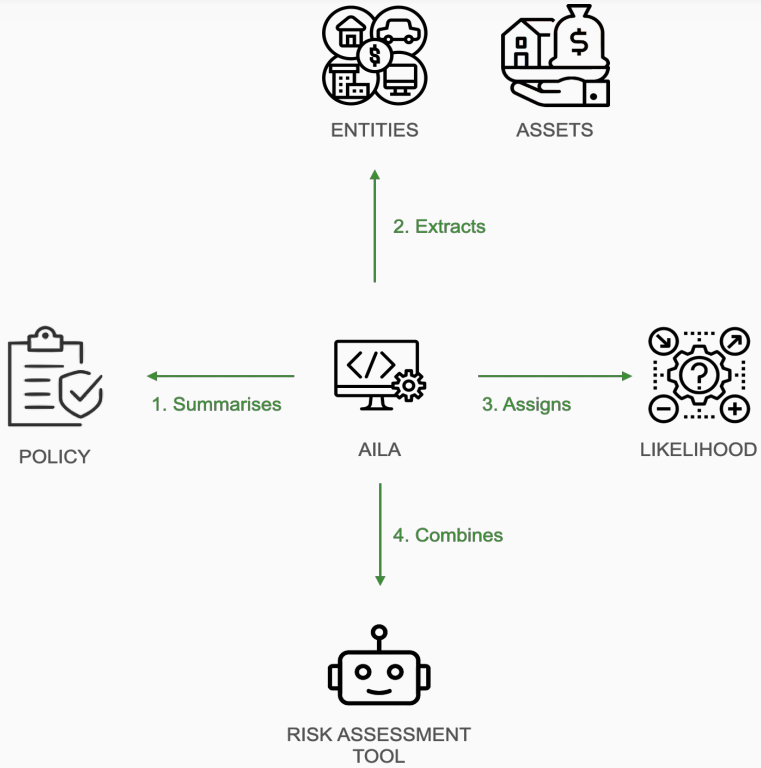
AILA aims at reducing the influence of ***subjectivity*** and ***distraction***.

AILA uses *Natural Language Processing* and *Machine Learning*.



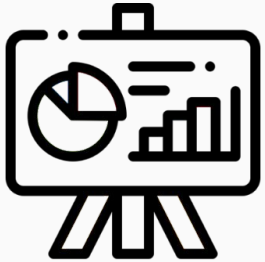
The process is also integrated with a *RA tool*.

Privacy Policy RA with AILA

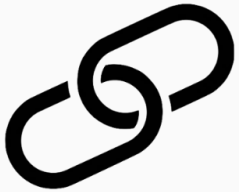


AILA in a Nutshell

1. AUTOMATED ASSET EXTRACTION

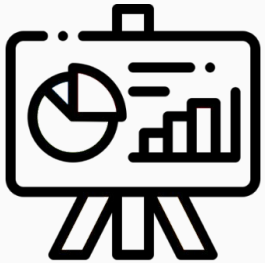


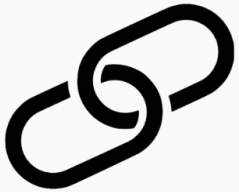
2. LIKELIHOOD DETERMINATION THROUGH AILA



3. COMBINED LIKELIHOOD DETERMINATION

AILA in a Nutshell

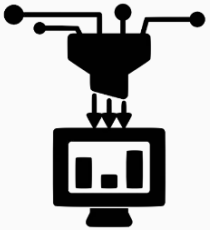




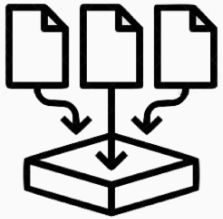
1. Automated Assets Extraction

This step is carried out by the **AILA Entity Extractor (AILAEE)**.

SUMMARISATION USING N-GRAMS



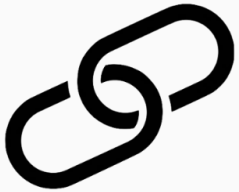
ENTITY RECOGNITION ALGORITHM



COLLECTION OF POLICY SENTENCES

AILA in a Nutshell

1. AUTOMATED ASSET EXTRACTION



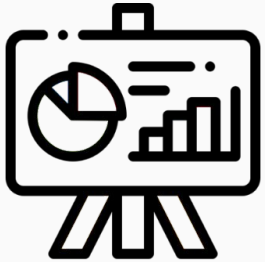
3. COMBINED LIKELIHOOD DETERMINATION

2. Likelihood Determination Through AILA

The **AILA Classifier (AILAC)** addresses this second challenge.

AILA in a Nutshell

1. AUTOMATED ASSET EXTRACTION



2. LIKELIHOOD DETERMINATION THROUGH AILA

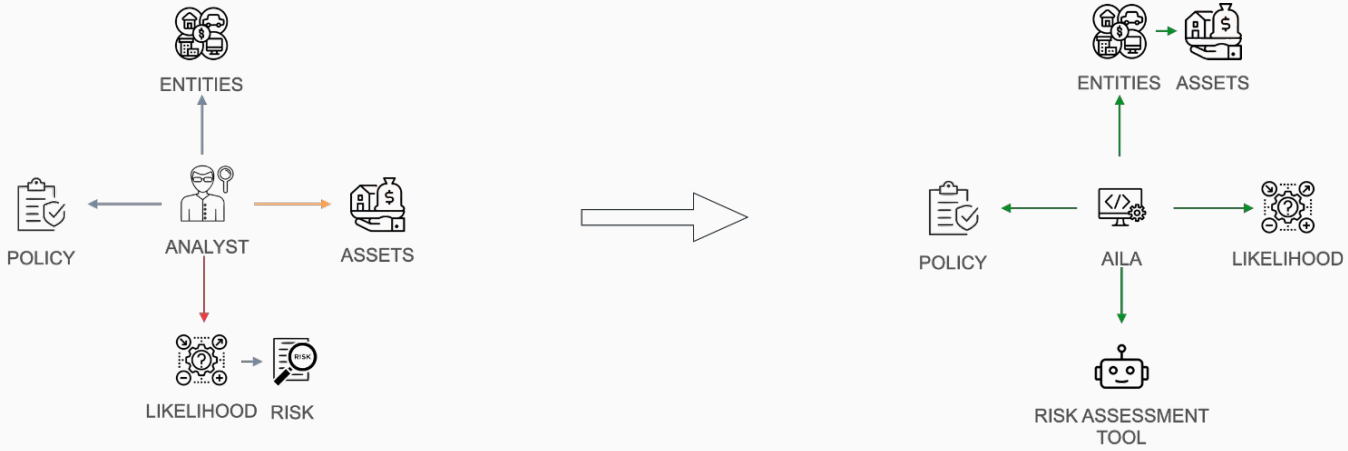
3. COMBINED LIKELIHOOD DETERMINATION

3. Combined Likelihood Determination

AILA Likelihood can be used to *sculpt* the Likelihood outputted by a standard tool on a specific privacy policy.

We combined AILA with *PILAR*.

What's the Deal in Short?



> AILA reduces **human subjectivity** through risk assessment.
> It facilitates **asset extraction** dramatically.
> It automates the **analyst's perception** of a policy.

Agenda

1. Intro to Privacy Risk Assessment
2. Intro to Privacy Threat Modelling
3. Embracing Approach
4. Combinatoric Approach
5. **AILA Methodology → Automotive Demo**
6. Conclusions

Automotive Demo

Toyota and **Mercedes** were the first two car brands in *Interbrand's 2020 Best Global Brands (BGB) Report.*

Tesla has a pioneer role on electric cars.

AILA Results

PILAR Class	AILA asset	PILAR Threat	Toyota Privacy Policy			Mercedes Privacy Policy			Tesla Privacy Policy		
			PILAR Likelihood	AILA Likelihood	Combined Likelihood	PILAR Likelihood	AILA Likelihood	Combined Likelihood	PILAR Likelihood	AILA Likelihood	Combined Likelihood
Software	Application	Hardware or software failure	3	4	3.6	3	3	3.1	3	4	3.6
		Software vulnerabilities	3			3			3		
		Defects in software maintenance / updating	4			4			4		
		Malware diffusion	3			3			3		
		Software manipulation	3			3			3		
Communication	Location	Accidental alteration of the information	3	5	4	3	3	3	3	3	3
		Information leaks	3			3			3		
		Unauthorised access	3			3			3		
		Traffic analysis	3			3			3		
		Deliberate alteration of information	3			3			3		
		Destruction of information	3			3			3		

RESULTS SAMPLE

AILA Validation

We validated AILA with a tool promoted by ENISA. Mercedes's privacy policy was chosen as test data.

Asset	AILA Fairness	AILA Likelihood		ENISA Likelihood
Geolocation	0.23	0.77	**High**	**High**
Maintenance	0.38	0.62	**Medium**	**High**
Vehicle Tracking System	0.4	0.6	**Medium**	**Medium**
System	0.1	0.9	**Very High**	**High**
Mobile Application	0.44	0.56	**Medium**	**Medium**
Payment Information	0.05	0.95	**Very High**	**High**
Data Collection	0.49	0.51	**Medium**	**Medium**

AILA AND ENISA LIKELIHOOD SAMPLES

AILA rocks!

$r = 0.93$

$r_s = 0.91$

$p - \text{value} = 0.00026$

Agenda

1. Intro to Privacy Risk Assessment
2. Intro to Privacy Threat Modelling
3. Embracing Approach
4. Combinatoric Approach
5. AILA Methodology
6. **Conclusions**

Conclusions

The risks for “*natural persons with regard to the processing of personal data and on the free movement of such data*” can be now assessed more precisely.

Future work includes:

- *deeper semantic analysis (semantic similarity and hypernym / hyponym)*
- *creation of a RA tool from scratch.*

Takeaways

– Subjectivity
+ Automation

Thanks for your attention!

For more information or questions:

mario.raciti@imtlucca.it – mario.raciti@phd.unict.it

https://tsumarios.github.io/

@tsumarios

https://linkedin.com/in/marioraciti

Non-malicious QR (maybe)