

# OWASP Top 10 Privacy Risks

Version 2.0 presented by Florian Stahl at the OWASP Stammtisch Hamburg

<https://owasp.org/www-project-top-10-privacy-risks/>

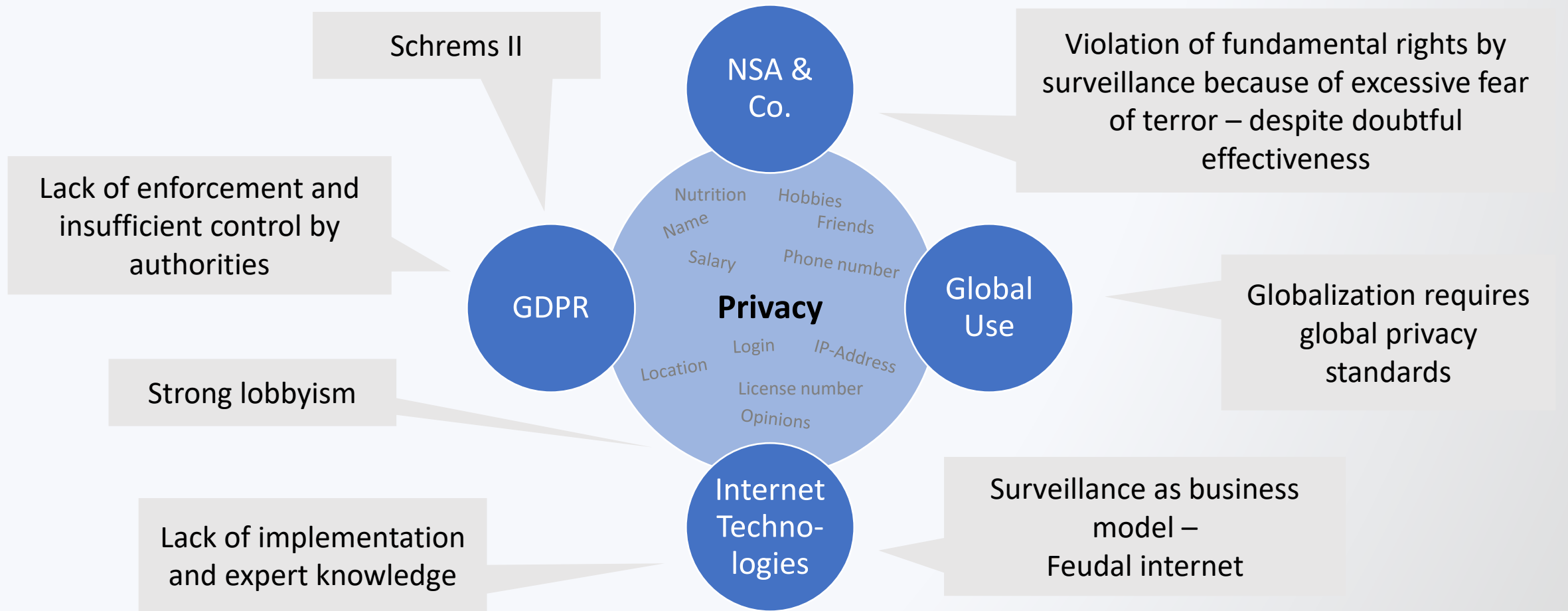
# About me

## Florian Stahl

- Principal Security Consultant @ msg Security Advisors (Munich / Regensburg)
- Dipl.-Winf., MSc, CISSP, CISM, CIPT
- 15 years of experience in information security & privacy (from pentester to team manager)
- Founder and Leader of the OWASP Top 10 Privacy Risks Project
- Hobbies: Family, tennis, snowboarding, travelling
- [florian.stahl@owasp.org](mailto:florian.stahl@owasp.org)



# Situation



# Top 10 Privacy Risks Project – Facts & Figures

- 2014 Foundation & Publication of version 1.0
- 2015 Member of IPEN (Internet Privacy Engineering Network)
- 2016 Publication of countermeasures
- 2021 Publication of version 2.0
- Currently working on countermeasures v2.0
- Available in 5 languages (soon in 7)
- OWASP Lab Project

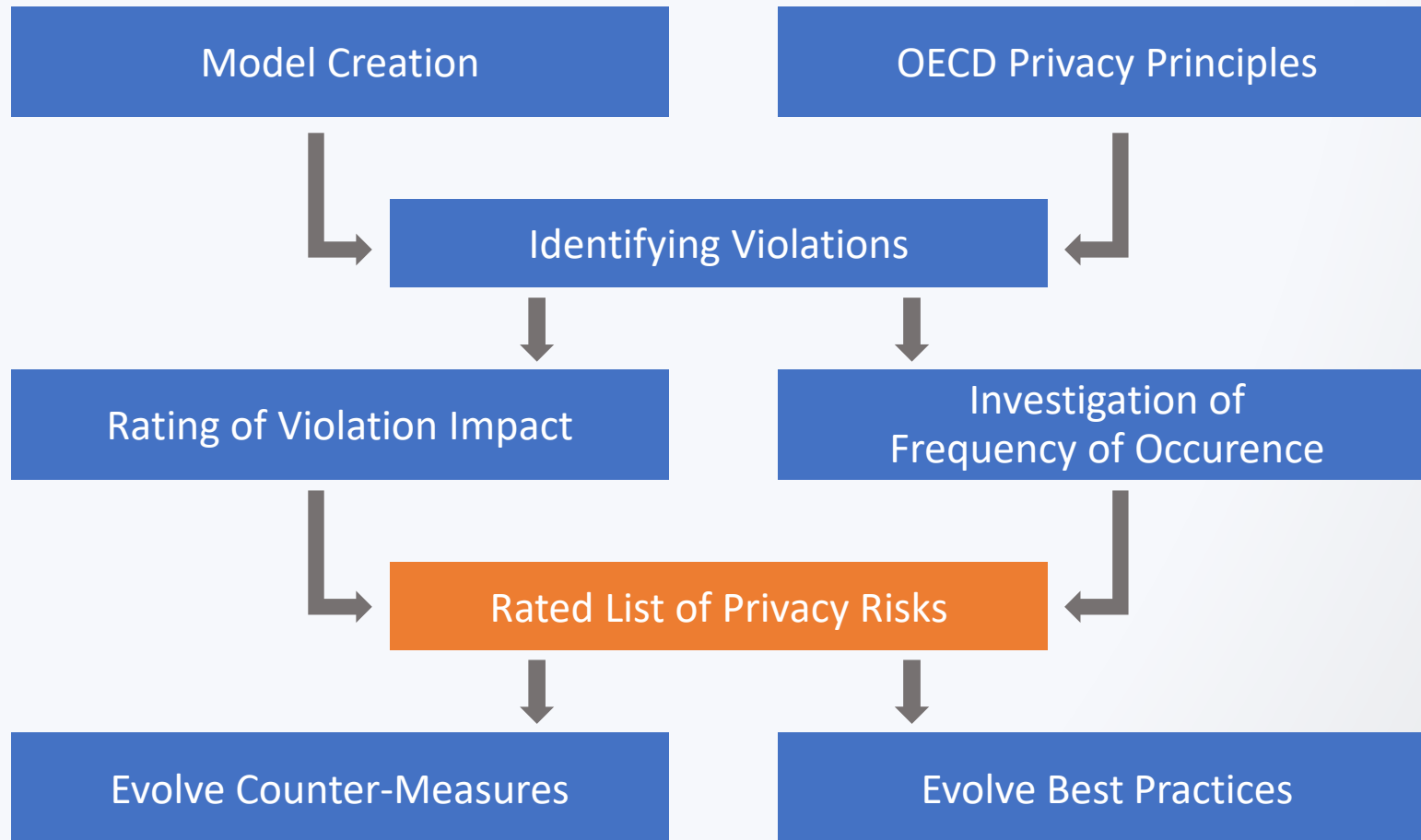


# Project Goal

- Identify the 10 most important **technical and organizational** privacy risks for web applications
- Provide transparency about privacy risks
- Independent from “local” laws based on OECD Privacy Principles
- Show countermeasures
- Educate developers, business architects and legal
- Not in scope: Self-protection for users

- 
1. Limitation of Collection
  2. Data Quality
  3. Specification of the Purpose
  4. Use Limitation
  5. Security
  6. Transparency
  7. Individual Participation
  8. Accountability

# Method (1/2)



# Method (2/2)

Survey to evaluate frequency of occurrence

- 60 privacy and security experts participated (62 in 2014)
- Rated 20 privacy violations for their frequency in web sites
- Slider instead of 4 radio buttons unexpectedly caused less differences

## Impact rating

Protection demand	Criteria for the assessment of protection demand				
	Application operator perspective		Data subject perspective		
	Impact on reputation and brand value	Financial loss	Social standing, reputation	Financial well being	Personal freedom
Low – 1	The impact of any loss or damage is <b>limited</b> and calculable.				
Medium – 2	The impact of any loss or damage is <b>considerable</b> .				
High – 3	The impact of any loss or damage is <b>devastating</b> .				

# Results Overview



## 2021 OWASP Top 10 Privacy Risks

2021	2014	Privacy Risks	Frequency	Impact	Type
1	1	⇒ Web application vulnerabilities	High	Very high	O
2	2	⇒ Operator-sided data leakage	High	Very high	O+T
3	3	⇒ Insufficient data breach response	High	Very high	O+T
4	New	☒ Consent on everything	Very high	High	O+T
5	5	⇒ Non-transparent Policies, Terms and Conditions	Very high	High	O
6	4	⇒ Insufficient deletion of personal data	High	High	O+T
7	New	☒ Insufficient data quality	Medium	High	O+T
8	9	↗ Missing or insufficient session expiration	Medium	Very high	T
9	13	↗ Inability of users to access and modify data	High	Very high	O+T
10	6	↘ Collection of data not required for the user-consented purpose	High	High	O

Type O: Organizational, T: Technical



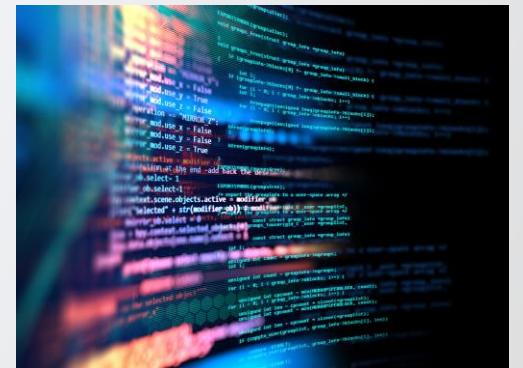
# P1: Web Application Vulnerabilities

## How to check?

- Are regular penetration tests performed (OWASP Top 10)?
- Are developers trained regarding web application security?
- Are secure coding guidelines applied?
- Is any of the used software out of date (server, DB, libs)?

## How to boost?

- Apply procedures like the Security Development Lifecycle
- Perform regular penetration tests by independent experts
- Install updates, patches and hotfixes on a regular basis



# P2: Operator-sided Data Leakage

## How to check?

- Research the reputation and reliability of the operator
- Audit the operator (before signing the contract or using it):
  - Paper-based audit (fair)
  - Interview-based audit (good)
  - On-site audit and system-checks (best)

## How to boost?

- Implement Awareness Campaigns
- Encrypt personal data
- Appropriate Identity & Access Management
- Strong Anonymization or Pseudonymization
- Further measures to prevent leakage of personal data (ISO 2700x)



# P3: Insufficient Data Breach Response

## How to check?

- Incident response plan in place?
- Plan tested regularly (request evidence like a test protocol)?
- Computer Emergency Response Team (CERT) / Privacy Team in place?
- Monitoring for incidents (e.g. SIEM) in place?

## How to boost?

- Create, maintain & test an incident response plan
- Continuously monitor for personal data leakage and loss
- Respond appropriately to a breach
  - Assign incident manager and incident response team
  - Notify data owners
  - ...



# P4: Consent on Everything \*New\*

## How to check?

- Is consent aggregated or inappropriately used to legitimate processing?
- Data flow restrictions rather than consent

## How to boost?

- Collect consent separately for each purpose (e.g. use of website and profiling for advertising).
- Consent should be voluntarily
- [Helen Nissenbaum on Post-Consent Privacy - YouTube](#)

**“Stop Thinking About Consent: It Isn’t Possible and It Isn’t Right”**

Dateneinstellungen verwalten

Alle akzeptieren

Picture sources: [Why Data Privacy Based on Consent Is Impossible \(hbr.org\)](#)  
& [www.facebook.com](http://www.facebook.com)

# P5: Non-transparent Policies, Terms & Conditions

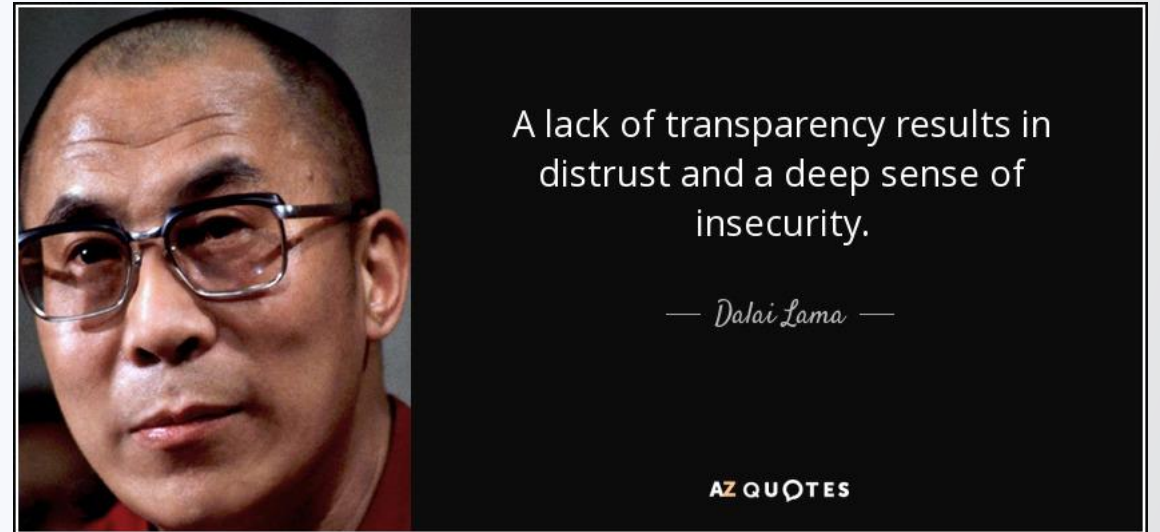
## How to check?

Check if policies, terms and conditions:

- Are easy to find and understandable for non-lawyers
- Fully describe data processing
  - Which data are collected, for what purpose, ...
  - In your language
- Complete, but KISS (Keep it short and simple)

## How to boost?

- Use a text analyzer, e.g.: <https://readable.com/>
- A short version of the T&Cs and pictograms can be used for easier understanding
- Use release notes to identify change history of T&Cs and policies/notices over time
- Deploy Do Not Track (W3C standard) and provide Opt-out



# P6: Insufficient Deletion of Personal Data

## How to check?

- Inspect the data retention or deletion policies / agreements.
- Evaluate their appropriateness
- Request deletion protocols
- Test processes for deletion requests

## How to boost?

- Delete personal data after termination of specified purpose
- Delete data on rightful user request
- Consider copies, backups and third parties
- Delete user profiles after longer period of inactivity

# P7: Insufficient Data Quality \*New\*

## How to check?

- Is it ensured that personal data is up-to-date and correct
- Check for possibilities to update personal data in the application
- Regular checks for validation, e.g. “Please verify your shipping address”
- Question how long it is likely that data is up to date and how often it usually changes

## How to boost?

- Provide an update form
- Ask user if his/her data is still correct
- Forward updated data to third parties / subsystems that received the user’s data before









# P8: Missing or Insufficient Session Expiration

## How to check?

- Is there an automatic session timeout < 1 week (for critical applications < 1 day).
- Is the logout button easy to find and promoted?

## How to boost?

- Configure to automatically logout after X hours / days or user-defined
- Obvious logout button
- Educate users

Where You're Logged In	
	Windows PC · Frankfurt, Germany Edge (Chromium Based) · <b>Active now</b>
	iPhone · Landshut, Germany Mobile Safari · 19 hours ago
	iPhone · Regensburg, Germany Mobile Safari · August 2 at 8:54 PM
	iPhone · Bad Abbach, Germany Mobile Safari · July 31 at 8:22 PM
	iPhone · Munich, Germany Mobile Safari · July 29 at 8:28 PM
	iPhone · Weiden in der Oberpfalz, Germany Mobile Safari · July 26 at 5:45 AM
	iPhone · Weiden in der Oberpfalz, Germany Mobile Safari · July 24 at 9:03 PM
	iPhone · Stephanskirchen, Germany Mobile Safari · July 23 at 12:07 PM

Picture source: facebook.com



# P9: Inability of users to access and modify data

## How to check?

- Do users have the ability to access, change or delete data related to them
- Are access, change or deletion requests processed timely and completely

## How to boost?

- Provide easy-to-use ways to access, change or delete data
- Appropriate Data Structure Model to handle user rights

# P10: Collection of data not required for the user-consented purpose

## How to check?

- Request description of purpose
- Check if collected data is required to fulfill the purpose
- If data is collected that is not required for the primary purpose(s), check if consent to collect and process this data was given and is documented
- Are individuals notified and asked if purpose or processing is changed?

## How to boost?

- Define purpose of the collection at the time of collection and only collect personal data required to fulfill this purpose
- Data minimization
- Option to provide additional data voluntarily to improve service (e.g. product recommendation, personal advertisement)

# Challenges in creating version 2.0

- Time, time, time ...
  - Work on version 2.0 began in the beginning of 2020 and was done more than one year later
- Coordinate a (new) virtual team of people with different background from all over the world
  - Few conference calls
  - Work in Google Docs
  - You need someone with the big picture and the goal in mind
- It was harder to find volunteers than in 2014 – privacy experts seem to be busier
- Overlaps between risks (e.g. P7 and P9) and abstraction level

# Next steps

- Translations (Chinese)
- Countermeasures v2.0
- Spread the word e.g. at:
- Apply in practice ;-)

