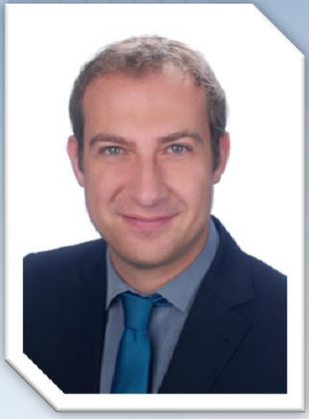
OWASP
Top 10 Privacy Risks Project

Covering privacy in web applications

OWASP AppSecEU 15
Amsterdam, The Netherlands

Who we are

Florian Stahl



- Lead Consultant for Information Security at msg systems
- MSc, CISSP, CIPT
- Project leader of the Top 10 Privacy Risks project
- Florian.Stahl@msg-systems.com

Stefan Burgmair

- Consultant for Information Security at msg systems
- Founded the Top 10 Privacy Risks as part

  of his Master's Thesis
- Stefan.Burgmair@msg-systems.com

.msg

OWASP AppSecEU 15
Amsterdam, The Netherlands

Agenda

1. Background
2. Goal
3. Method
4. Top 10 Risk List
5. Selected Countermeasures
6. Summary

What privacy is about

Privacy risks are related to personal data.

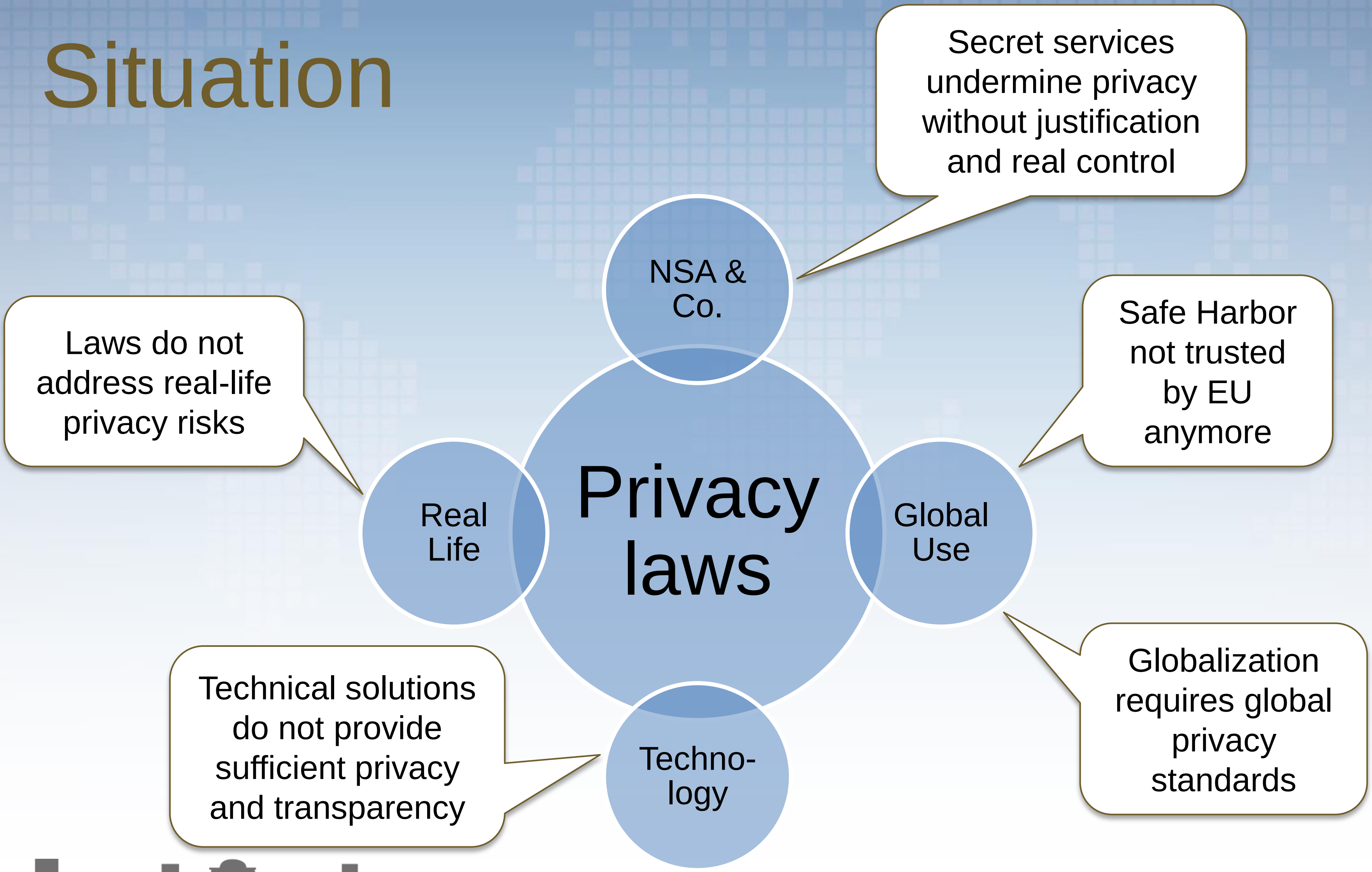
It is not only about Security, but also: *

- A Limitation of Collection
- Data Quality
- Specification of the Purpose
- Use Limitation
- Transparency
- Individual Participation

A privacy risk is a violation of these OECD Guidelines.

* According to the OECD Guidelines on the Protection of Privacy

Situation



Privacy laws

NSA & Co.

Secret services undermine privacy without justification and real control

Real Life

Laws do not address real-life privacy risks

Global Use

Safe Harbor not trusted by EU anymore

Globalization requires global privacy standards

Techno-logy

Technical solutions do not provide sufficient privacy and transparency

Forget about laws…

… we want **REAL PRIVACY** in web applications

- Currently many web applications contain privacy risks
- Anyway, they are compliant to privacy and data protection laws because
  - They are hosted in countries with poor privacy laws
  - Main focus on compliance, not on real-life risks for personal information
- No existing guidelines or statistical data about privacy risks in web applications
- Foundation of the OWASP Top 10 Privacy Risks Project in early 2014
- Nearly 100 privacy and security experts participated

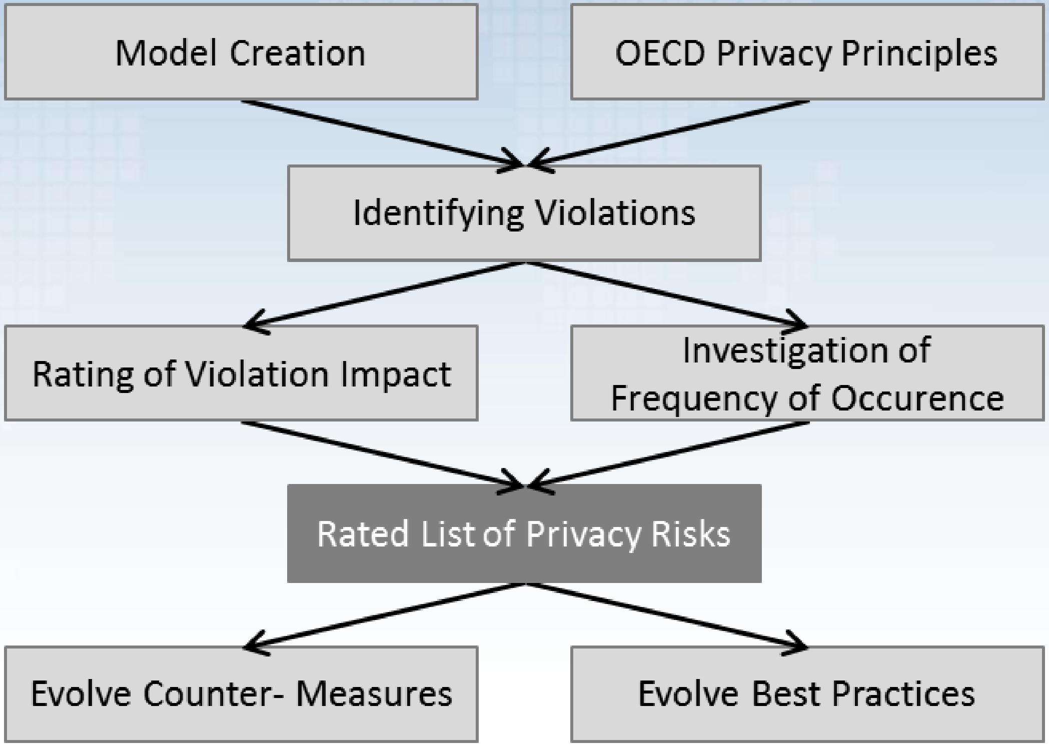
Project Goal

- Identify the most important **technical and organizational** privacy risks for web applications *
- Independent from local laws based on OECD Privacy Principles
- Focus on real-life risks for
  - User (data subject)
  - Provider (data owner)
- Help developers, business architects and legals to reach a common understanding of web application privacy
- Provide transparency about privacy risks
- Not in scope: Self-protection for users

* A privacy risk is a violation of the OECD privacy guidelines

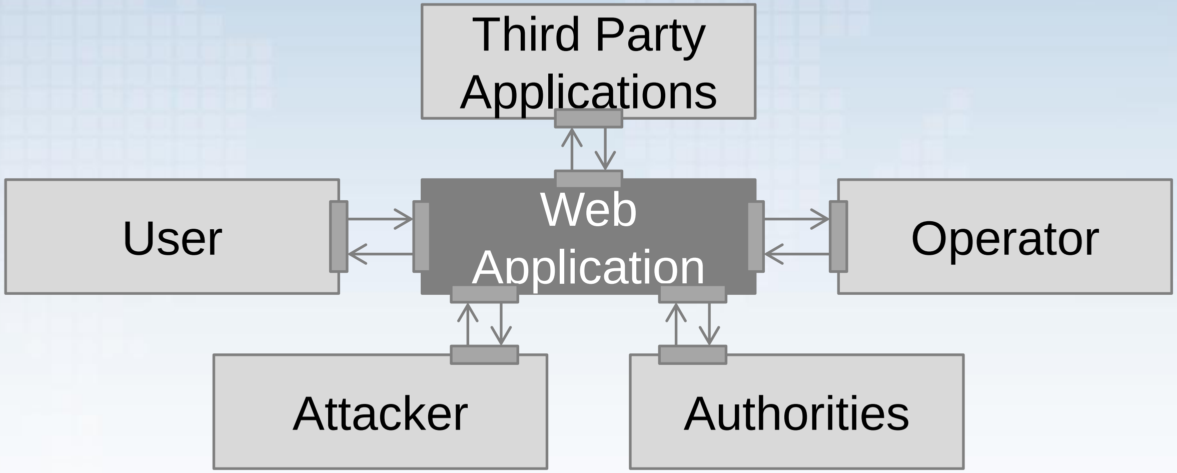
Project Method (1/4)

Approach of the project:



Project Method (2/4)

Five groups of actors are considered:

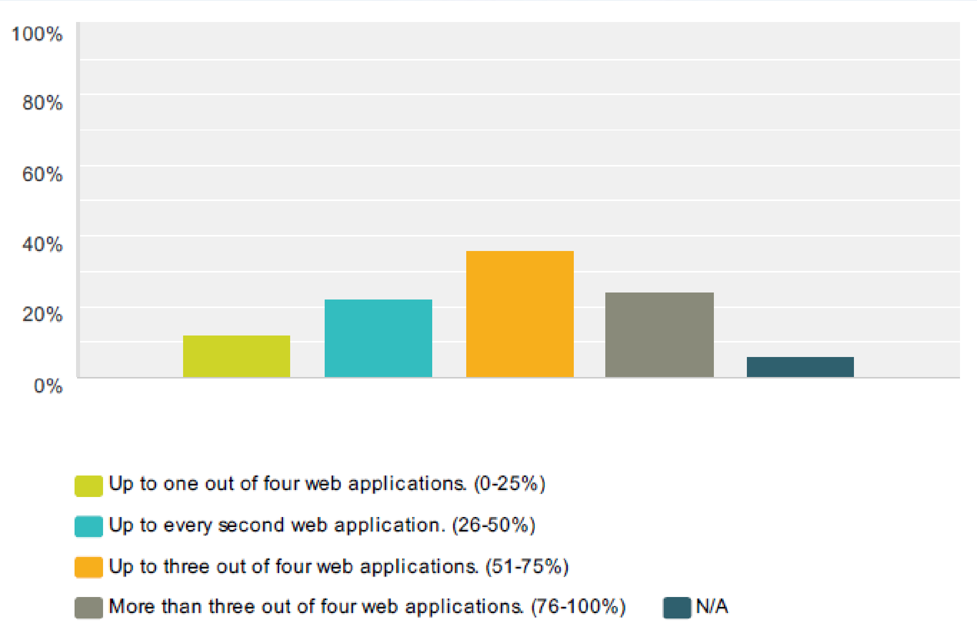


→ 20 privacy violations identified

Project Method (3/4)

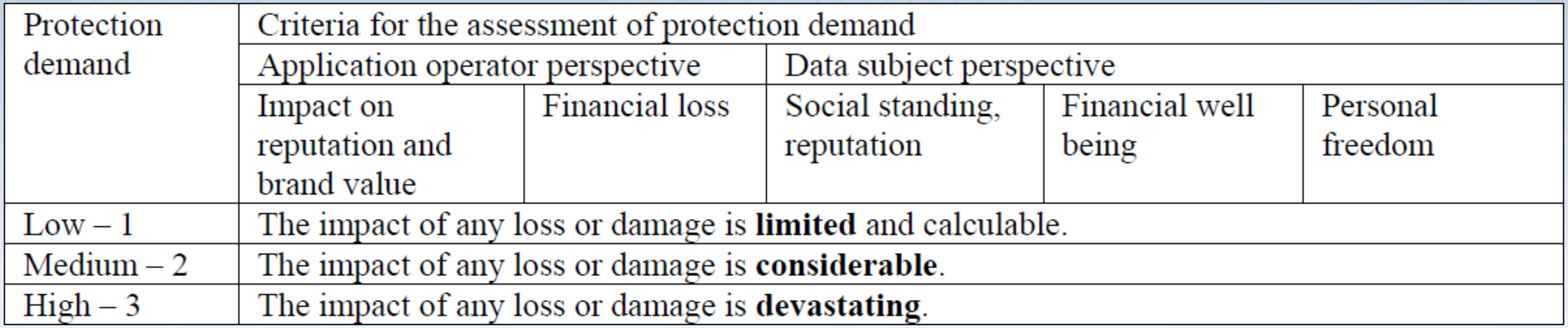
Survey to evaluate frequency of occurence

- 63 privacy and security experts participated
- Rated 20 privacy violations for their frequency in web sites
- Example: Sharing of data with third party (average 1.8)



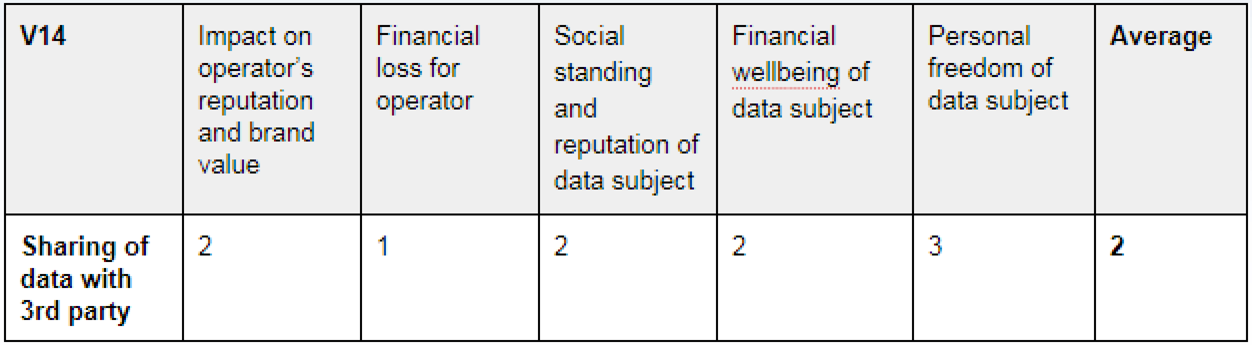
Project Method (4/4)

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 **limited** and calculable.				
Medium – 2	The impact of any loss or damage is **considerable**.				
High – 3	The impact of any loss or damage is **devastating**.				

Example:



V14	Impact on operator's reputation and brand value	Financial loss for operator	Social standing and reputation of data subject	Financial wellbeing of data subject	Personal freedom of data subject	**Average**
Sharing of data with 3rd party	2	1	2	2	3	**2**

Results: Top 10 Privacy Risks

P1 Web Application Vulnerabilities

P2 Operator-sided Data Leakage

P3 Insufficient Data Breach Response

P4 Insufficient Deletion of personal data

P5 Non-transparent Policies, Terms and Conditions

P6 Collection of data not required for the primary purpose

P7 Sharing of data with third party

P8 Outdated personal data

P9 Missing or Insufficient Session Expiration

P10 Insecure Data Transfer

Results: Top 10 Privacy Risks

P1 Web Application Vulnerabilities

P2 Operator-sided Data Leakage

P3 Insufficient Data Breach Response

P4 Insufficient Deletion of personal data

P5 Non-transparent Policies, Terms and Conditions

P6 Collection of data not required for the primary purpose

P7 Sharing of data with third party

P8 Outdated personal data

P9 Missing or Insufficient Session Expiration

P10 Insecure Data Transfer

P2: Operator-sided Data Leakage

Internal procedures or staff are often a reason for data leakage

Problems and Countermeasures:

- Poor access management and unnecessary copies of personal data
  - Implement a restrictive data access management for staff and externals
  - Data Leakage Prevention (DLP) solutions
  - Implement a data retention and deletion management
- Social engineering
  - Awareness campaigns
  - Establishing security protocols, policies and procedures for handling sensitive information

P2: Operator-sided Data Leakage

Another Problem: Anonymization of personal data

- Used for publication, research or usage inside and outside the operators organization
  - e.g. “We are using anonymized data for marketing purposes”
- Anonymization can be breached under specific circumstances
  - e.g. AOL search data leak
- Various types of data can be used to identify people
  - Through background knowledge and comparison tables
  - An unique identifier based on e.g. location data or device configuration
  - 87 % of the US-citizens (216 million of 248 million) are uniquely identifiable according to their {5-digit ZIP-code, gender, date of birth} *

* L. Sweeney, Simple Demographics Often Identify People Uniquely

P5: Non-transparent Policies, Terms & Conditions

☑ "I have read and agree to the terms and conditions"
Is the **Biggest Lie** on the web.
I confessed
BiggestLie.com

Problems:

- Privacy Policies, Terms & Conditions are
  - not up-to-date, inaccurate, incomplete or hard to find
  - and they do not support rational decision making[1]
- Conditions are too long and users do not read them
  - It would require 244 hours / year to read the online privacy policies of every visited website[1]
- Data processing is not explained sufficiently

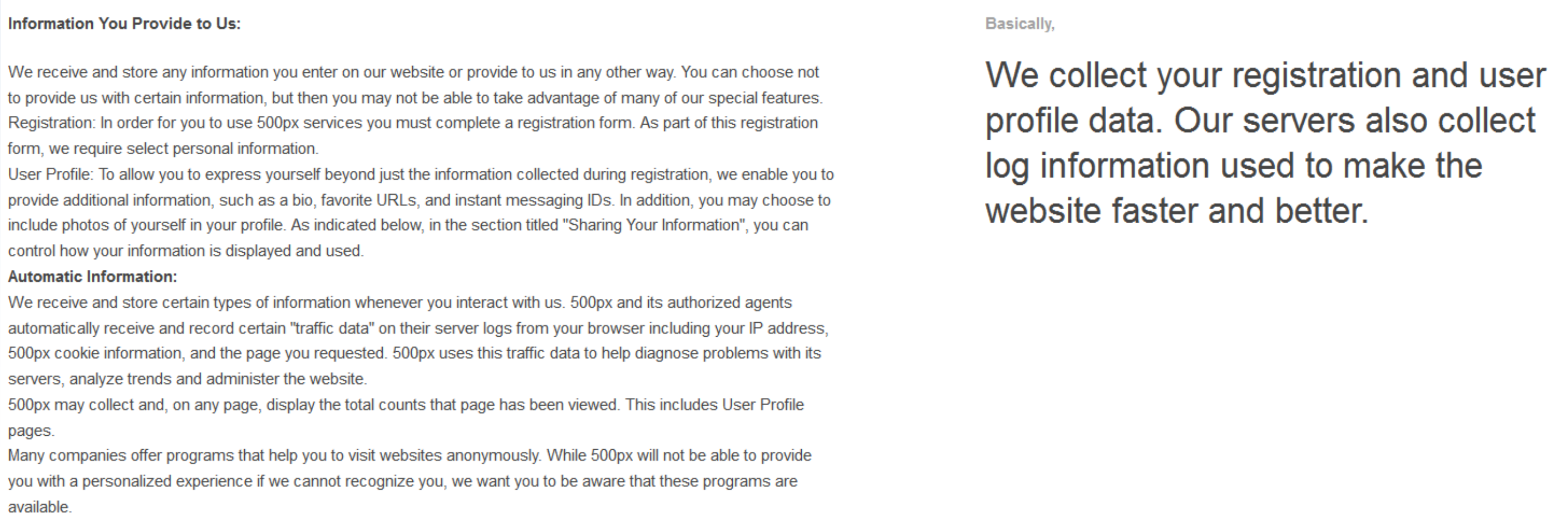
[1] from The Cost of Reading Privacy Policies A. McDonald, L. Cranor

* Picture source: BiggestLie.com

P5: Non-transparent Policies, Terms & Conditions

Countermeasures

- Point out where to find the privacy related policies
- Use pictograms for visual aid
- Add succinct and understandable summaries of legal paragraphs:



Information You Provide to Us:

We receive and store any information you enter on our website or provide to us in any other way. You can choose not to provide us with certain information, but then you may not be able to take advantage of many of our special features.
Registration: In order for you to use 500px services you must complete a registration form. As part of this registration form, we require select personal information.
User Profile: To allow you to express yourself beyond just the information collected during registration, we enable you to provide additional information, such as a bio, favorite URLs, and instant messaging IDs. In addition, you may choose to include photos of yourself in your profile. As indicated below, in the section titled "Sharing Your Information", you can control how your information is displayed and used.

Automatic Information:

We receive and store certain types of information whenever you interact with us. 500px and its authorized agents automatically receive and record certain "traffic data" on their server logs from your browser including your IP address, 500px cookie information, and the page you requested. 500px uses this traffic data to help diagnose problems with its servers, analyze trends and administer the website.
500px may collect and, on any page, display the total counts that page has been viewed. This includes User Profile pages.
Many companies offer programs that help you to visit websites anonymously. While 500px will not be able to provide you with a personalized experience if we cannot recognize you, we want you to be aware that these programs are available.

Basically,

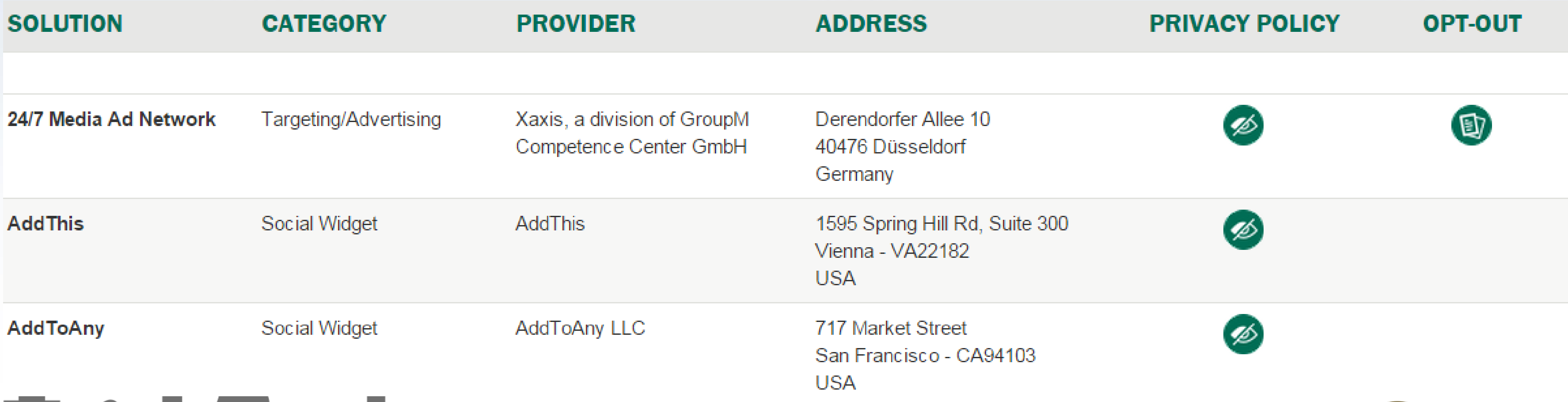
We collect your registration and user profile data. Our servers also collect log information used to make the website faster and better.

* Picture source: https://500px.com/privacy

P5: Non-transparent Policies, Terms & Conditions

Countermeasures

- In case of an update of the conditions:
  - Keep track of which user gave consent to which version
- Make the conditions available in every relevant language
- Provide transparency about third parties:



SOLUTION	CATEGORY	PROVIDER	ADDRESS	PRIVACY POLICY	OPT-OUT
24/7 Media Ad Network	Targeting/Advertising	Xaxis, a division of GroupM Competence Center GmbH	Derendorfer Allee 10 40476 Düsseldorf Germany	●	●
AddThis	Social Widget	AddThis	1595 Spring Hill Rd, Suite 300 Vienna - VA22182 USA	●	
AddToAny	Social Widget	AddToAny LLC	717 Market Street San Francisco - CA94103 USA	●	

* Picture source: http://www.kaspersky.com/third-party-tracking

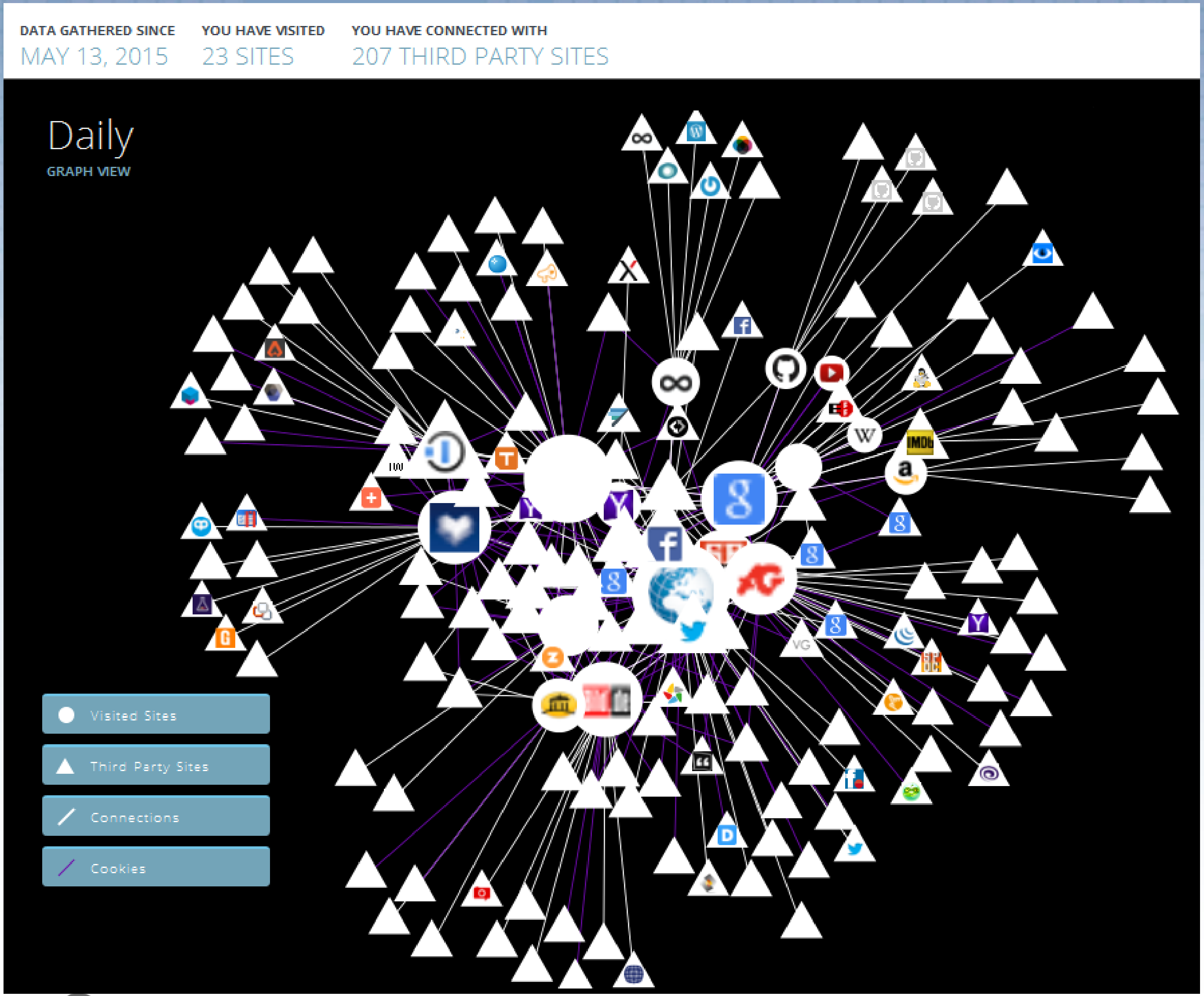
P7: Sharing of Data with 3rd Party

Third Parties:

- Advertisers, Subcontractors, etc.
- Used for Analytics, Video integration, Maps, Social networks, etc.

Problems:

- Data is transferred or sold to third parties without user’s knowledge and consent
- Complete loss of control



DATA GATHERED SINCE
MAY 13, 2015

YOU HAVE VISITED
23 SITES

YOU HAVE CONNECTED WITH
207 THIRD PARTY SITES

Daily
GRAPH VIEW

● Visited Sites

▲ Third Party Sites

/ Connections

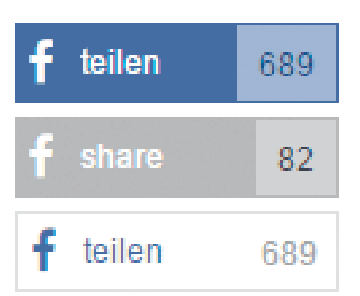
/ Cookies

* Picture source: LightBeam (Addon for Firefox)

P7: Sharing of Data with 3rd Party

Countermeasures

- Third party services should not be used per default if it is not required (e.g.: shariff for social network buttons[1])
- Masking of data before transfer if possible
- Development of a Third Party Monitoring Strategy:
  - Gateway release for third party content (whitelist or blacklist)
  - Contractual arrangements regarding Policies, Data usage, …
  - Monitoring of user complaints



ct SHARIFF

[1] https://github.com/heiseonline/shariff

* Picture source: heise.de

P9: Missing or Insufficient Session Expiration

Companies try to track the user behavior as long as possible, e.g.

- Social Network
- Search engine
- Leading webshop

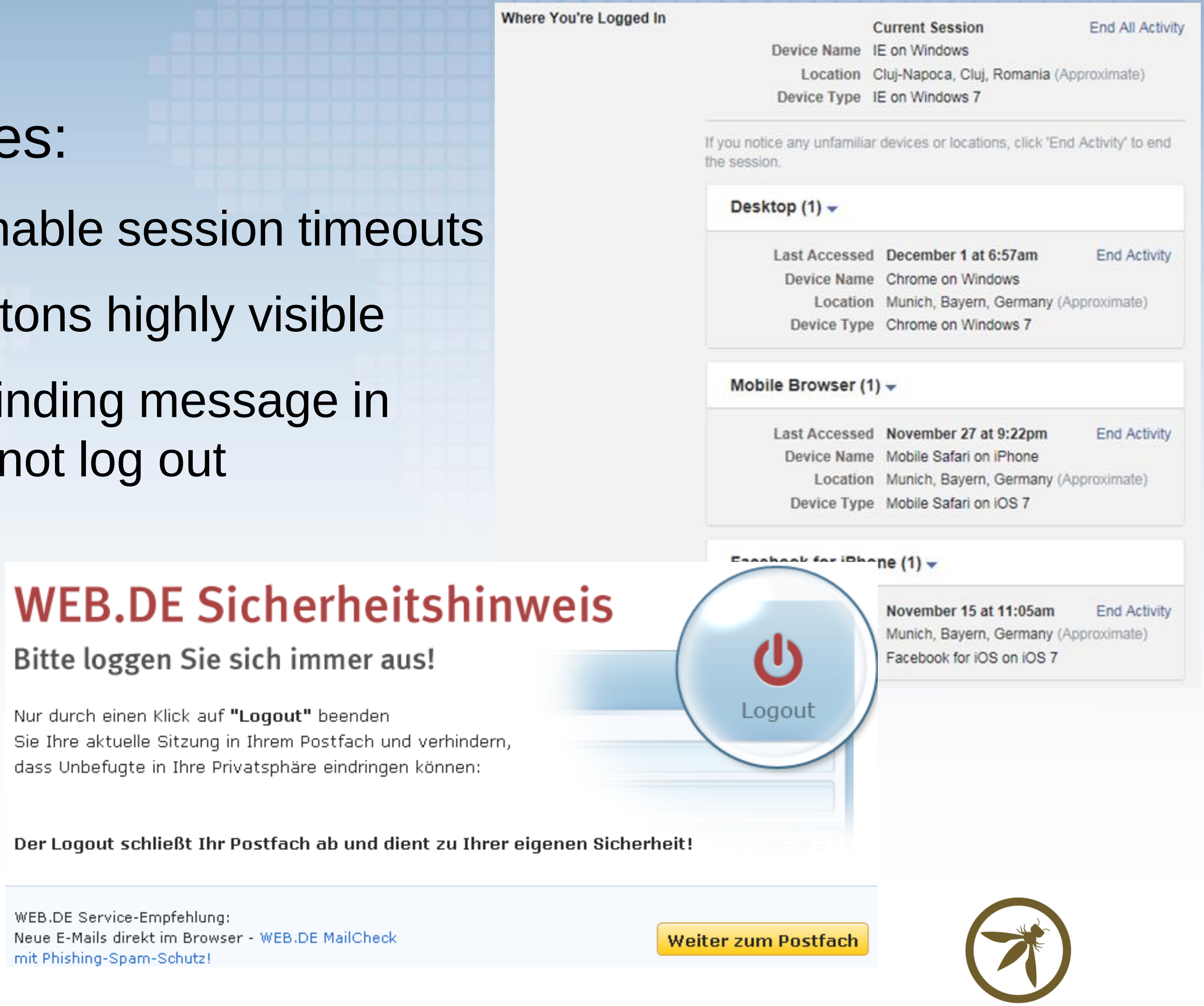
Problem:

- Users are not aware about the collection of their data
- Missing logout might raise security issues

P9: Missing or Insufficient Session Expiration

Countermeasures:

- Usage of reasonable session timeouts
- Make logout buttons highly visible
- Generate a reminding message in case a user did not log out



Where You're Logged In

	Current Session	End All Activity
Device Name	IE on Windows	
Location	Cluj-Napoca, Cluj, Romania (Approximate)	
Device Type	IE on Windows 7	

If you notice any unfamiliar devices or locations, click 'End Activity' to end the session.

Desktop (1)

Last Accessed	December 1 at 6:57am	End Activity
Device Name	Chrome on Windows	
Location	Munich, Bayern, Germany (Approximate)	
Device Type	Chrome on Windows 7	

Mobile Browser (1)

Last Accessed	November 27 at 9:22pm	End Activity
Device Name	Mobile Safari on iPhone	
Location	Munich, Bayern, Germany (Approximate)	
Device Type	Mobile Safari on iOS 7	

Facebook for iPhone (1)

November 15 at 11:05am — End Activity
Munich, Bayern, Germany (Approximate)
Facebook for iOS on iOS 7

WEB.DE Sicherheitshinweis

Bitte loggen Sie sich immer aus!

Nur durch einen Klick auf **"Logout"** beenden Sie Ihre aktuelle Sitzung in Ihrem Postfach und verhindern, dass Unbefugte in Ihre Privatsphäre eindringen können:

Der Logout schließt Ihr Postfach ab und dient zu Ihrer eigenen Sicherheit!

WEB.DE Service-Empfehlung:
Neue E-Mails direkt im Browser - WEB.DE MailCheck mit Phishing-Spam-Schutz!

Picture sources: facebook.com, web.de

Summary

- Privacy in many web applications should be improved
- Lack of awareness regarding privacy risks
- No practical guidance on how to avoid privacy risks so far
- OWASP Top 10 Privacy Risks project created to address those issues and educate developers and lawyers
- The project identifies technical and organizational risks independent from local laws
- Try to consider these risks when implementing or auditing web applications and apply countermeasures!

Further information

- OWASP Top 10 Privacy Risks Project: https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project

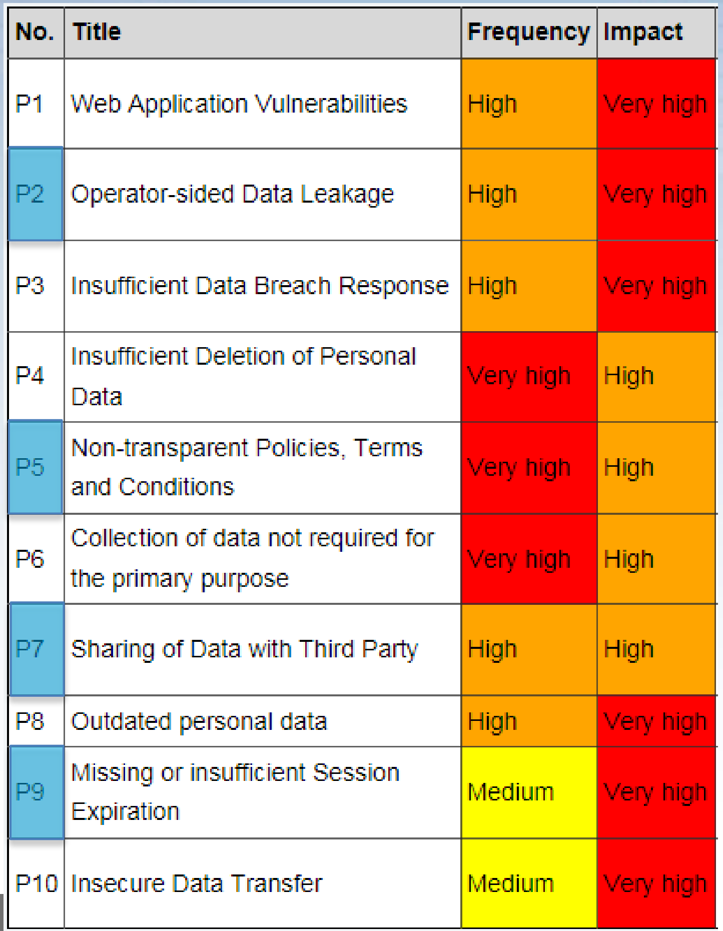
  → Feel free to contribute

- Internet Privacy Engineering Network (IPEN): https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/IPEN

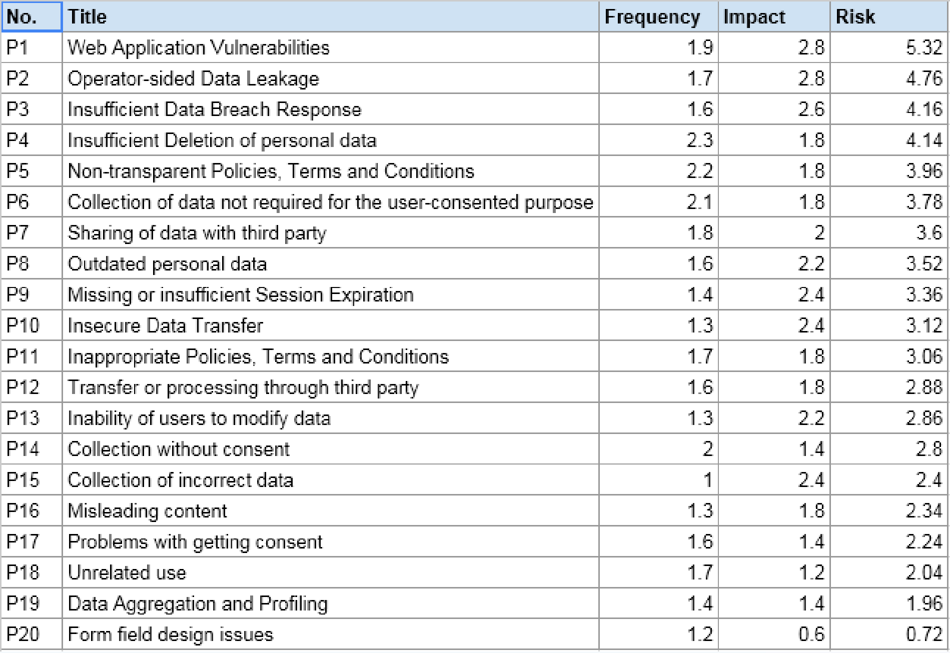
- Project sponsor: http://www.msg-systems.com

- Florian Stahl's personal blog: http://securitybydesign.de/

Results in detail



No.	Title	Frequency	Impact
P1	Web Application Vulnerabilities	High	Very high
P2	Operator-sided Data Leakage	High	Very high
P3	Insufficient Data Breach Response	High	Very high
P4	Insufficient Deletion of Personal Data	Very high	High
P5	Non-transparent Policies, Terms and Conditions	Very high	High
P6	Collection of data not required for the primary purpose	Very high	High
P7	Sharing of Data with Third Party	High	High
P8	Outdated personal data	High	Very high
P9	Missing or insufficient Session Expiration	Medium	Very high
P10	Insecure Data Transfer	Medium	Very high



No.	Title	Frequency	Impact	Risk
P1	Web Application Vulnerabilities	1.9	2.8	5.32
P2	Operator-sided Data Leakage	1.7	2.8	4.76
P3	Insufficient Data Breach Response	1.6	2.6	4.16
P4	Insufficient Deletion of personal data	2.3	1.8	4.14
P5	Non-transparent Policies, Terms and Conditions	2.2	1.8	3.96
P6	Collection of data not required for the user-consented purpose	2.1	1.8	3.78
P7	Sharing of data with third party	1.8	2	3.6
P8	Outdated personal data	1.6	2.2	3.52
P9	Missing or insufficient Session Expiration	1.4	2.4	3.36
P10	Insecure Data Transfer	1.3	2.4	3.12
P11	Inappropriate Policies, Terms and Conditions	1.7	1.8	3.06
P12	Transfer or processing through third party	1.6	1.8	2.88
P13	Inability of users to modify data	1.3	2.2	2.86
P14	Collection without consent	2	1.4	2.8
P15	Collection of incorrect data	1	2.4	2.4
P16	Misleading content	1.3	1.8	2.34
P17	Problems with getting consent	1.6	1.4	2.24
P18	Unrelated use	1.7	1.2	2.04
P19	Data Aggregation and Profiling	1.4	1.4	1.96
P20	Form field design issues	1.2	0.6	0.72