OWASP
Open Web Application Security Project

Top 10 Privacy Risks in Web Applications

IAPP Global Privacy Summit 2015

5 March 2015, Washington DC

Florian Stahl (Project Lead, msg systems, Germany)

.msg
Sponsored by

About me

Florian Stahl

- Master's degree in Information System Science with Honors (University of Regensburg, Germany)
- Master's degree in Computer Science (Växjö University, Sweden)
- CIPT, CISSP, CCSK

Working with information security & privacy for more than 8 years:

- Security & Privacy Consultant at Ernst & Young
- Lead Consultant Information Security, msg systems in Munich
- Project Lead OWASP Top 10 Privacy Risks Project

Goal: Interdisciplinary and holistic understanding of information security and privacy in organizations

Hobbies:

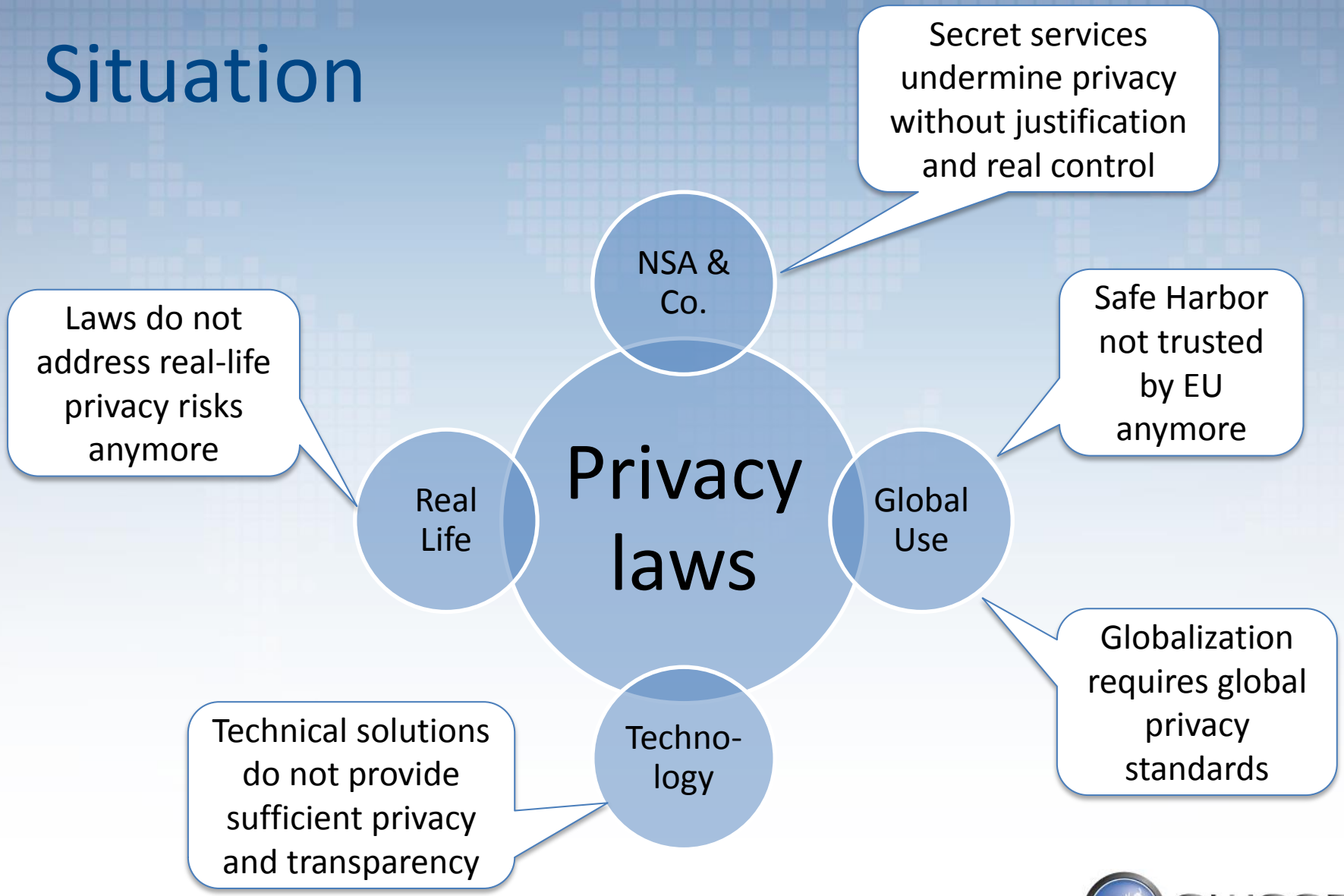
- Wife and son
- Travelling, mountain biking, snowboarding

OWASP
Open Web Application Security Project

Agenda

1. Situation
2. Top 10 Privacy Risks Project
    a. Background
    b. Goal
    c. Method
    d. How would you rate?
    e. Results
3. Countermeasures
4. Summary

Situation



Sponsored by .msg

OWASP Open Web Application Security Project

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 legal to reach a common understanding of web application privacy
- Provide transparency about privacy risks
- Not in scope: Self-protection for users

OWASP

Open Web Application Security Project

- Community dedicated for web application security
- Open source and non-profit organization
- Creates freely-available articles, methodologies, documentation, tools, and technologies
- Known for its Top 10 Security risk list (established standard) and other projects
- Provides platform for the Top 10 Privacy Risks project

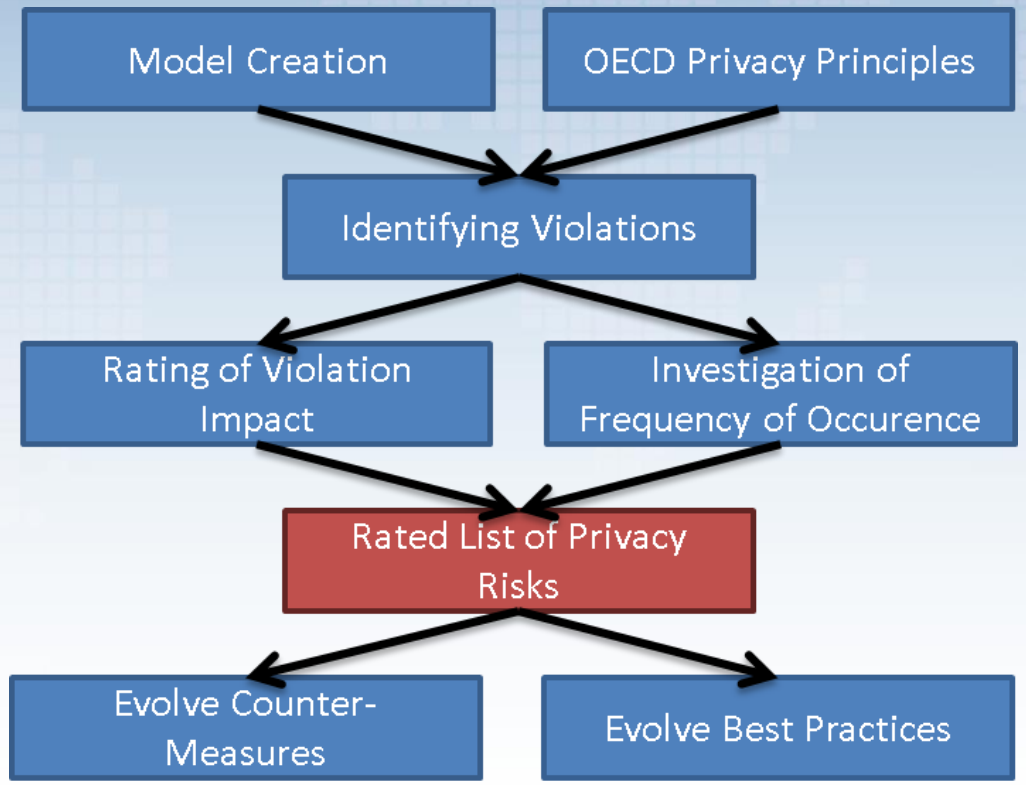
Member of IPEN

Internet Privacy Engineering Network

- Founded in 2014 by EU Data Protection Supervisor's Head of Policy
- Goal to bring together privacy experts with developers

OWASP
Open Web Application Security Project

Project Method (1/3)



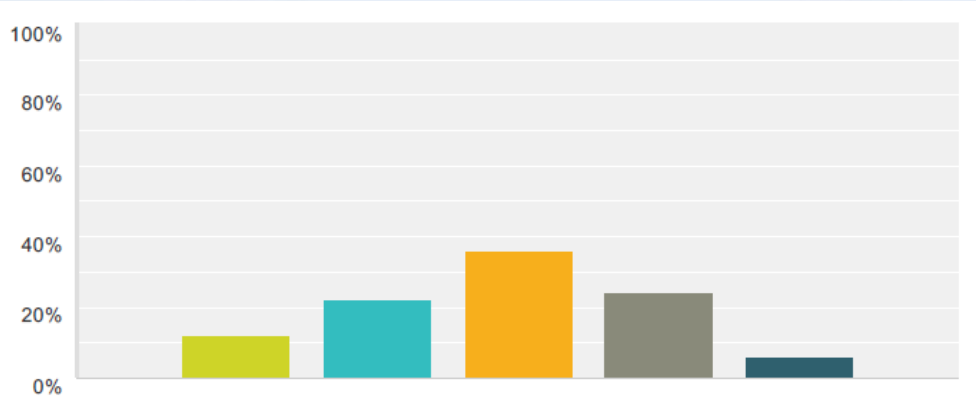
Sponsored by

OWASP Open Web Application Security Project

Project Method (2/3)

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)



OWASP
Open Web Application Security Project

Project Method (3/3)

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**

OWASP Open Web Application Security Project

Privacy Risks: How would you rate?

a. Non-transparent Policies, Terms and Conditions
b. Insufficient Data Breach Response
c. Outdated personal data
d. Sharing of data with third party
e. Operator-sided Data Leakage
f. Missing or Insufficient Session Expiration
g. Insufficient Deletion of personal data
h. Insecure Data Transfer
i. Collection of data not required for the primary purpose
j. Web Application Vulnerabilities

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 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

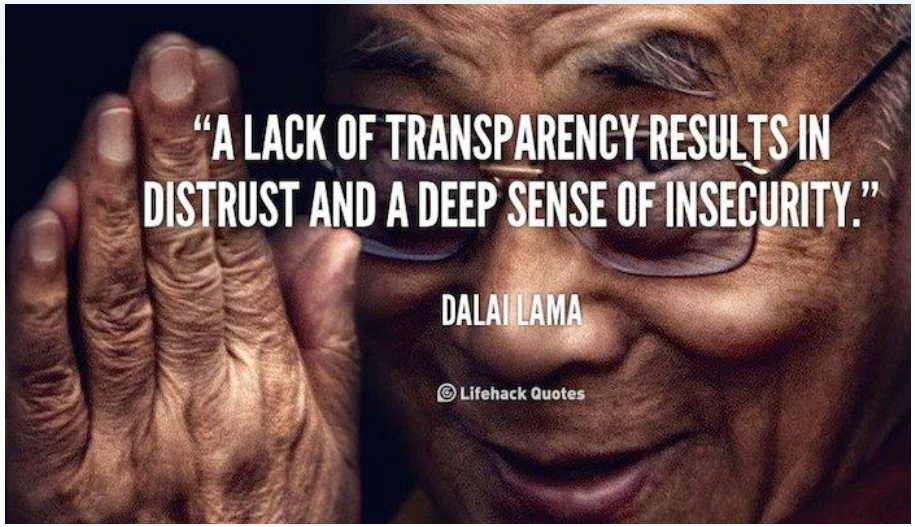
P2: Operator-sided Data Leakage

Internal procedures or staff are often a reason for data leakage

- Poor access management
- Lack of awareness
- Unnecessary copies of personal data
- Weak anonymization of personal data:
  - For publishing or using inside the company: e.g. “We are using anonymized data for marketing purposes.”
  - Anonymization can go wrong: e.g. AOL search data leak
  - Location data, browsing behavior or device configuration can be used to identify people

P5: Non-transparent Policies, Terms & Conditions

- Privacy Policies, Terms & Conditions are not up-to-date, inaccurate, incomplete or hard to find
- Data processing is not explained sufficiently
- Conditions are too long and users do not read them



Sponsored by .msg

OWASP Open Web Application Security Project

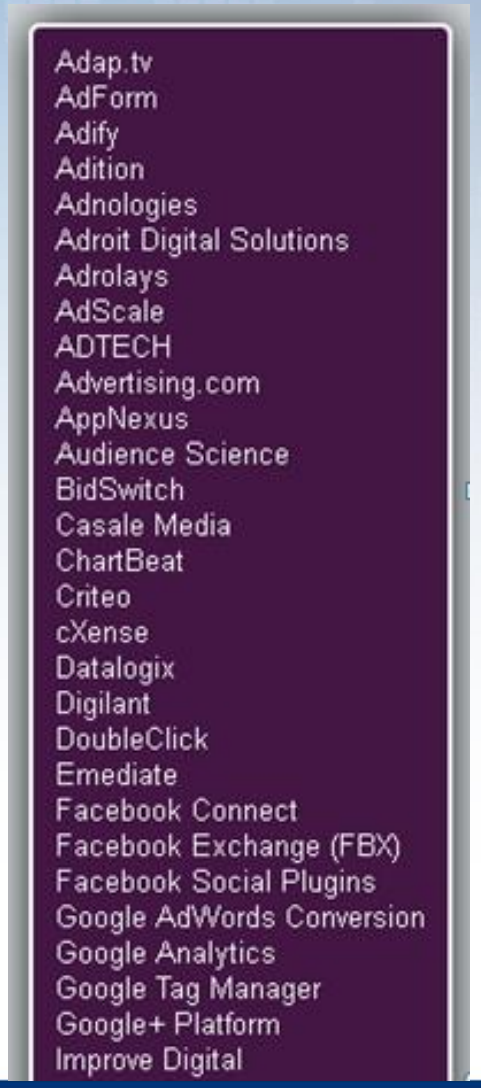
P7: Sharing of Data with 3rd Party

Third Parties:

- Advertisers
- Subcontractors
- Video integration
- Maps
- Social networks

Problems:

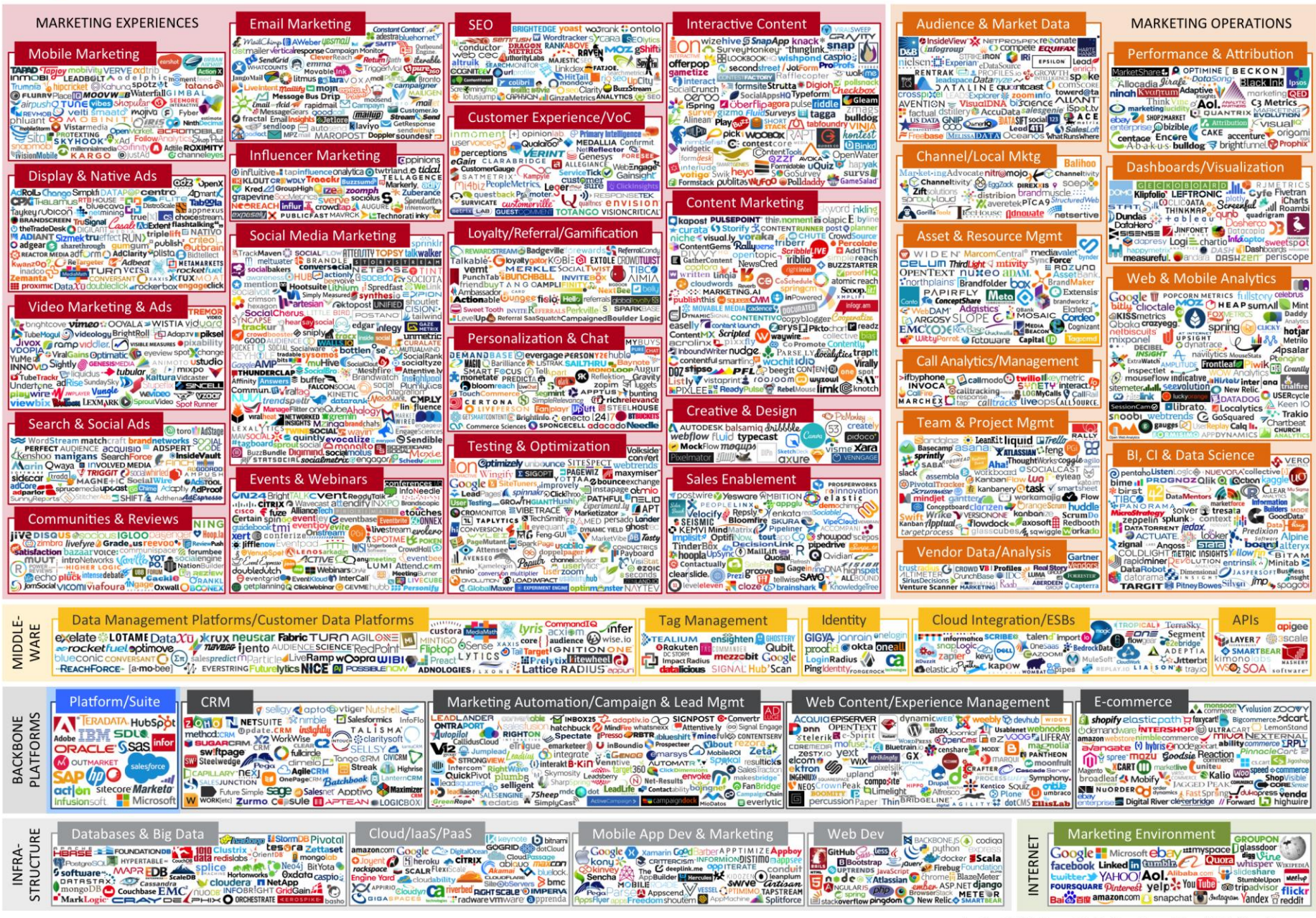
- Data is transferred or sold to third parties without user's knowledge and consent
- Complete loss of control



Picture source: Ghostery

chiefmartec.com Marketing Technology Landscape

January 2015



by Scott Brinker @chiefmartec http://chiefmartec.com

P9: Missing or Insufficient Session Expiration

Automatic session timeout and a highly visible logout button is security state-of-the-art, not for:

- Google
- Facebook
- Amazon

Picture sources: facebook.com, web.de

Countermeasures (1/4)

Raise **Awareness** among:

- Product / Application Designers (business)
  - They decide about functionality that affects privacy
- Developers / IT
  - Sometimes have the choice to implement privacy friendly applications
- Data Protection / Legal
  - Personal information is mainly processed in IT systems
  - IT has to be considered when implementing privacy programs
- Questions:
  - How many of you have a legal background?
  - How many of you consider web applications in their privacy programs?

Countermeasures (2/4)

Implement **processes**

- That consider privacy in all development stages from requirements analysis to implementation (preventive)
- To audit privacy measures in web applications (detective)

Ask simple **questions**

- Did you consider privacy when designing the application?
- Did you address the OWASP Top 10 Privacy Risks?
  - How are privacy incidents handled?
  - How is data deleted?
  - How do you avoid vulnerabilities in the application?
  - …

Countermeasures (3/4)

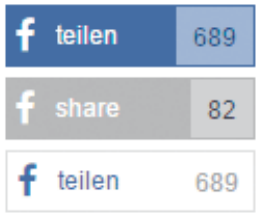
Technology examples

- Avoid Data Leakage
  - Restrictive Access Management
  - Awareness campaigns
  - Strong anonymization techniques
  - Data Leakage Prevention (DLP) solutions
- Improve session timeout
  - Configure to automatically logout after X hours / days
  - Obvious logout button
  - Educate users

Countermeasures (4/4)

Technology examples

- Ideas for better transparency in terms & conditions
  - Text analyzer: readability-score.com
  - HTTPA: http with accountability developed by MIT
- Share data with third party on click only
  - Youtube embedded video: Enhanced privacy mode
  - Facebook buttons: heise Shariff



Picture source: heise.de

Summary

- Currently there are many privacy risks in web applications
- Compliance-based approach does not cover all of them
- Lack of awareness regarding real-life privacy risks
- OWASP Top 10 Privacy Risks project created to address this issue 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
- My personal blog: http://securitybydesign.de/