OWASP
Open Web Application Security Project

How to Boost Web Application Privacy

IAPP Privacy Intensive 2016

20 April 2016, London

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 9 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:

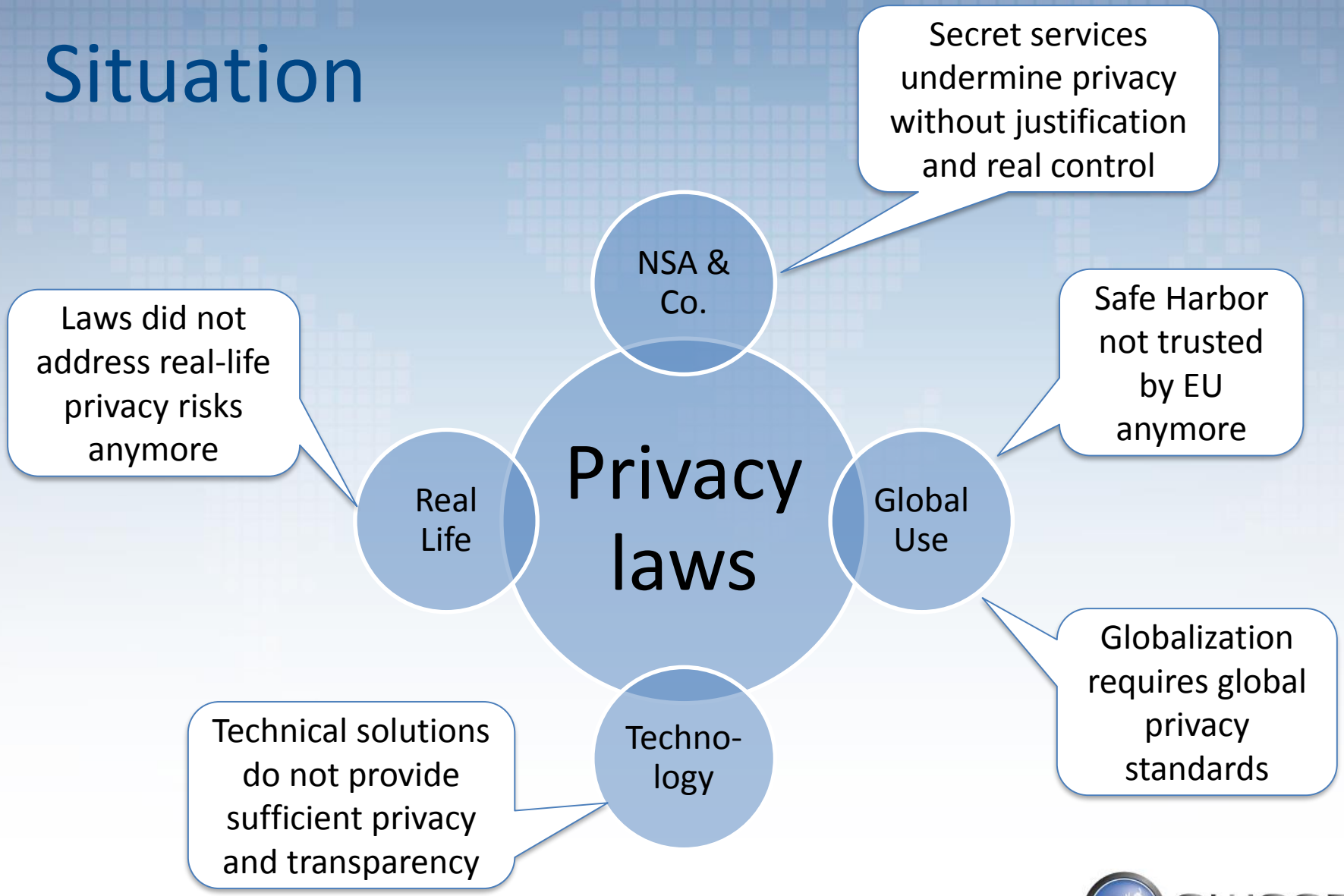
- Wife and son
- Travelling, mountain biking, snowboarding

OWASP
Open Web Application Security Project

Agenda

1. Situation
2. Top 10 Privacy Risks Project
    a. Goal
    b. Method
    c. Results
3. Countermeasures – how to check & boost
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 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

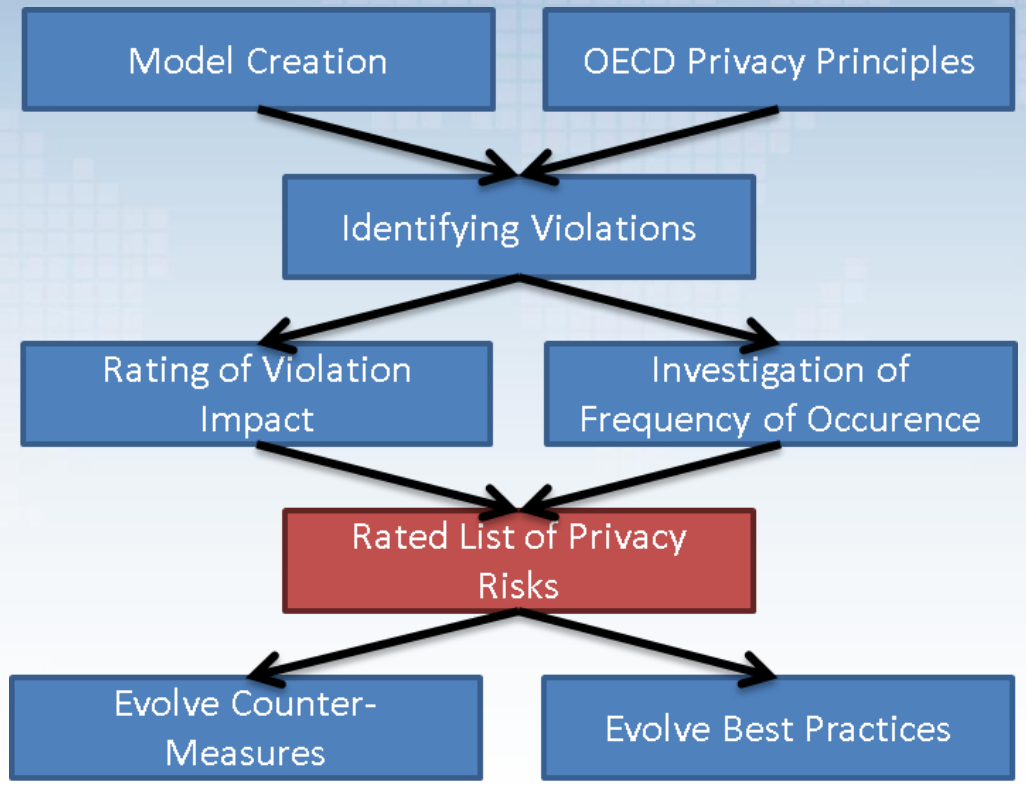
- Community dedicated for web application security
- Open source and non-profit organization
- Creates freely-available articles, methodologies, documentation, tools, and technologies
- Known for its Top 10 Security risk list (established standard) and other projects
- Provides platform for the Top 10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

Project Method



Sponsored by

OWASP Open Web Application Security Project

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

How to check & boost?

OWASP
Open Web Application Security Project

P1: Web Application Vulnerabilities

How to check?

- Are regular penetration tests performed focusing on privacy?
- Are developers trained regarding web application security?
- Are secure coding guidelines applied?
- Is any of the used software out of date (server, DB, libraries)?

How to boost?

- Apply procedures like the Security Development Lifecycle (SDL)
- 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
  - …

OWASP Open Web Application Security Project

P4: 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

P5: Non-transparent Policies, Terms and Conditions

How to check?

Check if policies, terms and conditions:

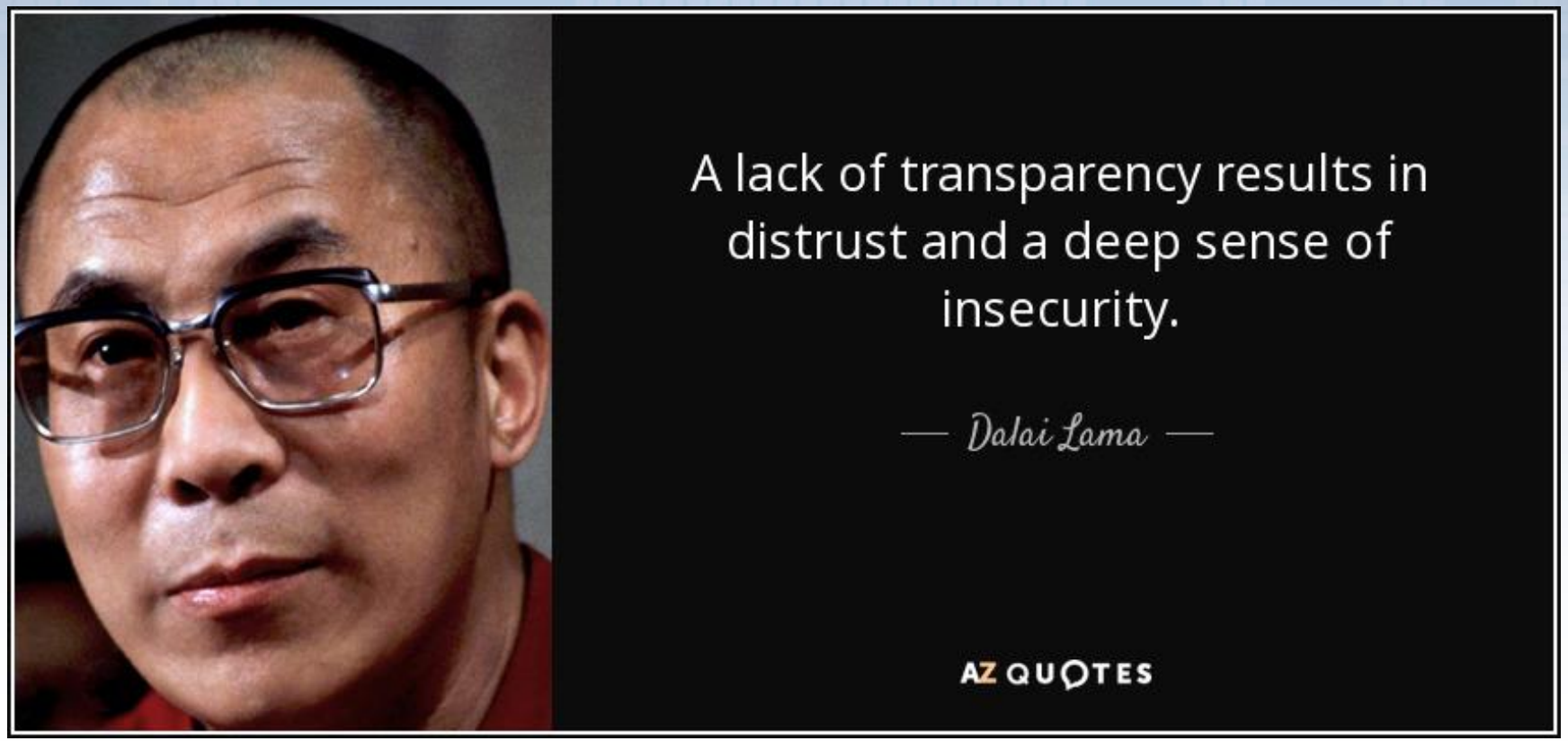
- Are easy to find and understandable for non-lawyers
- Fully describe data processing
  - Which data are collected, for what purpose, …
  - In your language
- Complete, but KISS (Keep it short and simple)

How to boost?

- Use a text analyzer: readability-score.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

OWASP
Open Web Application Security Project

P5: Non-transparent Policies, Terms & Conditions



P6: Collection of data not required for the primary purpose

How to check?

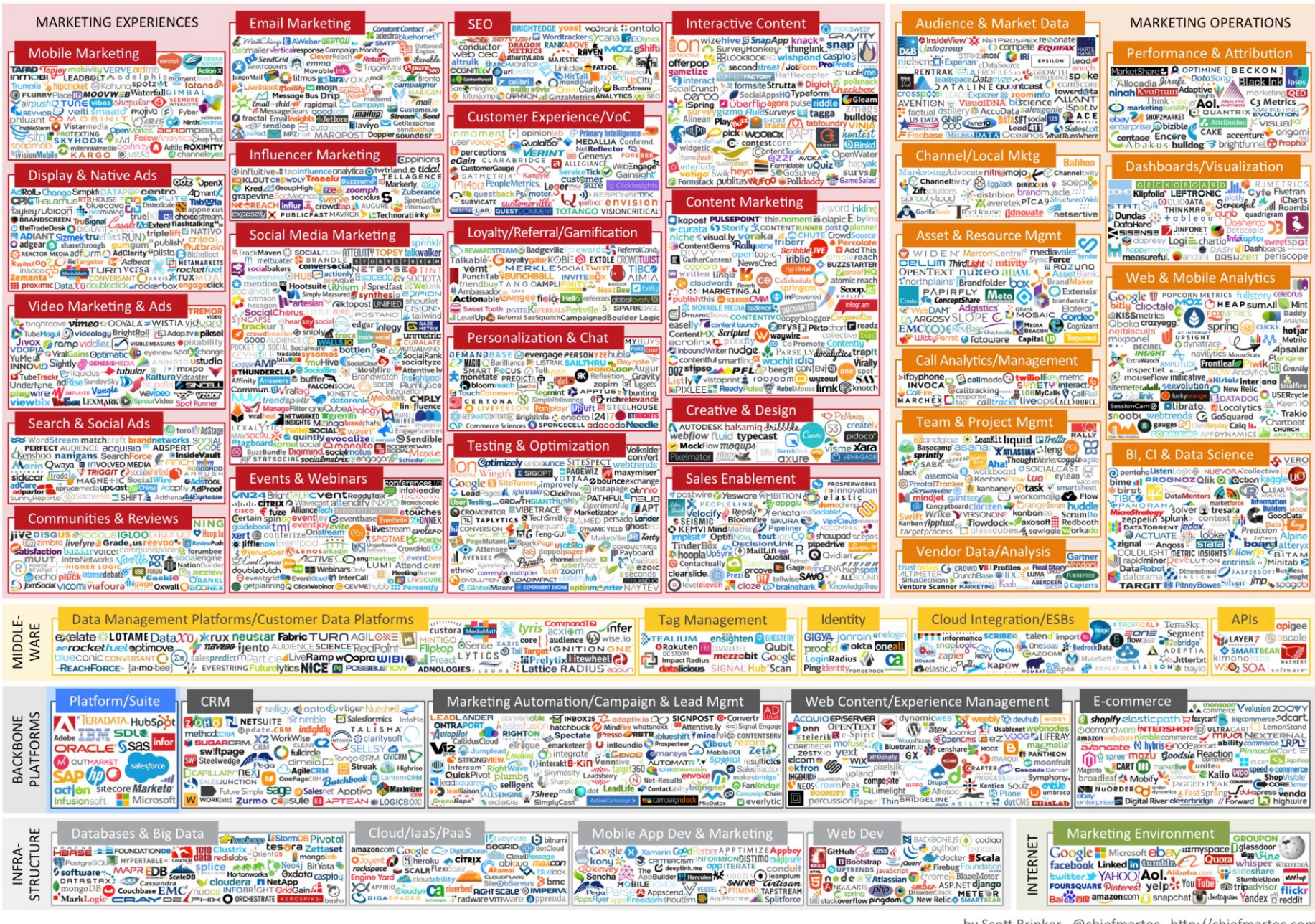
- Request description of purpose
- Check if collected data is required to fulfill the purpose
- If data is collected that is not required for the primary purpose(s), check if consent to collect and process this data was given and is documented
- Are individuals notified and asked if purpose or processing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

chiefmartec.com Marketing Technology Landscape

January 2015



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

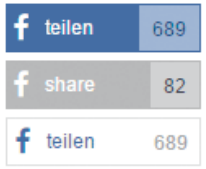
P7: Sharing of Data with 3rd Party

How to check?

- Are third party solutions in use (plugins, buttons, maps, videos, advertising, etc.), which ones and what personal data is transferred?
- Is third party tracking disclosed (which third parties and what data)?
- Are third parties rated and checked regarding privacy?
- Is privacy and handling of personal data part of the contract and if yes, what restrictions are in place?

How to boost?

- Use third party content only where required, not by default
- Develop a Third Party Monitoring Strategy
- Use privacy friendly solutions like
  - Social networks buttons that only send data on click (heise Shariff)
  - Youtube enhanced privacy mode
  - …



heise Shariff: https://github.com/heiseonline/shariff

P8: Outdated personal data

How to check?

- Is it ensured that personal data is up-to-date
- 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

OWASP
Open Web Application Security Project

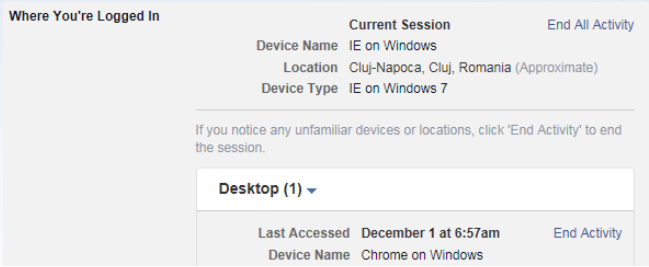
P9: Missing or Insufficient Session Expiration

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



Picture sources: facebook.com, web.de

P10: Insecure Data Transfer

How to check?

- Is data encrypted during transfer?
- Are secure protocols and algorithms used?
- Are privacy-friendly protocols available for transfer?
- Are private protocols enforced where appropriate? (E.g. Login only available over HTTPS, and sensitive records only accessible by TLS or SFTP)

How to boost?

- See how to check
- Technically, e.g.:
  - Use Privacy Extensions in IPv6
  - Support TLS/DTLS, do not support SSLv3

OWASP
Open Web Application Security Project

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/