

# How to Boost Web Application Privacy

## **IAPP Privacy Intensive 2016**

20 April 2016, London

Florian Stahl (Project Lead, msg systems, Germany)



# 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:

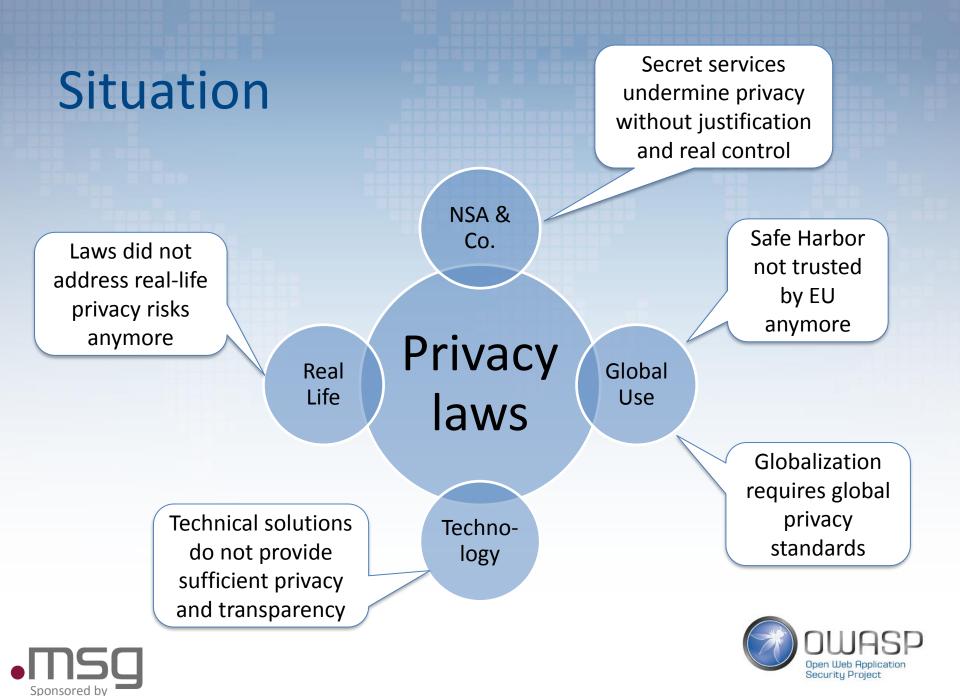
- Wife and son
- Travelling, mountain biking, snowboarding



# Agenda

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





## 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**

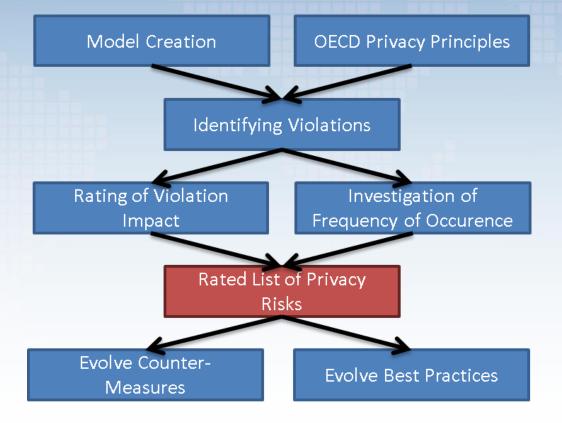
- Founded in 2014 by EU Data Protection Supervisor's Head of Policy
- Goal to bring together privacy experts with developers







# **Project Method**







# 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?





## **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)?

- 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)

- 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?

- 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: 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

- 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)

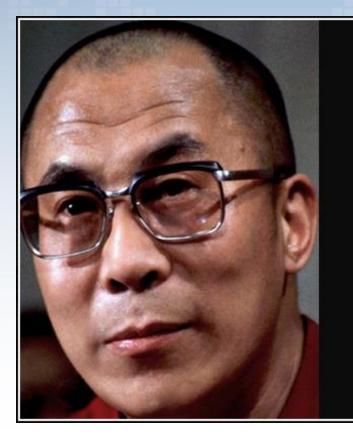
- Use a text analyzer: readability-score.com
- A short version of the T&Cs and pictograms can be used for easier understanding
- Use release notes to identify change history of T&Cs and policies/notices over time
- Deploy Do Not Track (W3C standard) and provide Opt-out







## P5: Non-transparent Policies, Terms & Conditions



A lack of transparency results in distrust and a deep sense of insecurity.

Dalai Lama

AZQUOTES





# 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?

- 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

MARKETING OPERATIONS

Performance & Attribution

ADGALSENERT A OPTIMINE [ BECKON]
Algent Adaptive
Algent Adaptive
A

Dashboards/Visualization

#### MARKETING EXPERIENCES

#### Mobile Marketing

To Action X TAPAD Tapiov mobivitu VERV Trumpia hipcricket & del phic moment and Trumpia hipcricket & Kahung spotz et tatance european and the spotz et tatance argument argument and the spotz et tatance argument ar PLUMRYPBOCIE MOOVW EWAterhalle I M B AL airpush O'Line (ress should be all the should be all SILO SKYHOOK Ad Follo

#### Display & Native Ads

CC2: OpenX CC2: O

#### Video Marketing & Ads

brightcove vineo: OVALA = WISTIA viduor Tubehogu videology BrightRoll Adopt v piksel Jivoz (many videology brightRoll Adopt v UVDPIA Valcans Optimetre overview spitchings Vublez Sightly coststered verview subuling interview size was subuling and spitchings interview size was verview spitchings verview size was verview size was subuling verview size was verview size was verview size was subuling verview size was vervie

#### Search & Social Ads

MIDDLI WARE

> LLI. UCTURE

> STRI

WordStream matchcraft brandretwork Mable Reference Autorical and Autorial Stream and Autorial address proceedings and Autorial Au

# Email Marketing Walk Larp Meder (2570) Sender Verlagespore Company Forder Movable Sender Verlagespore Methods Sender Verla

#### Social Media Marketing

CRACTOR MUDA adf. Jmm O Adclarity Polston Outbrain Manazogo Cracing Addedity Polston Outbrain Indica Converse Call Converse Ca Hootsuite Lithurn Spredfast hexagon Tractesan - Coktopost United CISION: SocialChorus, The Bird Postano tailwind NCAPSE - bear of social - edgar infegy COOR ALD LEVE OF STIPLY A FORT INTERNATION OF Correction of the section of the sec Inity Answers Stationsocal Chiegration Intrum. By Tailoo KINETIC KINETIC Kinetic Chiegration Kinetic Chiegrat Commun. Manageritier of Psuccesphotogy
Manageritie Sendible

#### Events & Webinars conferences of

SEO BRIGHTEDGE yoast worrank tontolo Contractor and the sector of t Clarity BuzzSt eeemingtrog troiling to the second se

#### Customer Experience/VoC

ioment [+] opinio

Personalization & Chat Mini Bailla SE Cleverage Arson vzehube
Mini Bailla SE Cleverage Arson vzehube
Shart Fecus O tellupar
Montate Pecus O tellupar
Montate Pecus

#### Testing & Optimization

On Optimizely unbounce SITESPECT we con//ed Vingity SIGOPT PAGEWIZ maxymiser Communities & Reviews
Communities
Communities & Reviews
Communities
Communiti





	Creative & Design	Dic Monkey
i	AUTODESK balsamig dribble	(57) create
١	webflow fluid typecast 👝 🥨	pidoco"
ę	MockFlow moqups	visme Xara
ł	Pixelmator JIIII axure	

#### Sales Enablement

postwire Vesware AMBITION elastic Velocity - Report - Constant - Constant



MORTH LEAT TUREO alami, AssetBankaer PAPIR FLY Metro Control Control MacControl Control Control MacControl Control Control MacControl Control MacControl Control MacControl Control MacControl Control

#### Call Analytics/Management

>ifbyphone Callmodo twilloll evenetric INVOCA Callmodo Swill The The interaction Callmod Callmod Callmod Action (Callmod A R C H & Callmod Callmod Viveops (ALLSource

Sondoloz . LeanKit liquid Trello Bascondo e leastit liquid Wrell ReLLY Bascondo e leastit liquid Wrell RelLY saak as an in the same in the source of the same sack assemble Karbonico LLO e view is an mindje same and the same as a same as a same with the same and the same as a same as a same basis of the same and the same as a same as a same to the same and the same as a same as a same as a same to the same and the same as a same as a same as a same to the same and the same as a same as

#### Vendor Data/Analysis

Gartner LUSTRALIUS CROWD VB | Profiles | Red Story Wandows SiriusDecisions ARKETING Rad ARKETING CONTRAL ARKETING



Data Management Platforms/Customer Data Platforms

#### Tag Management







INTERNET





Volkside



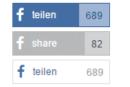
Marketing Environment	
	ce glassdoor
Google Microsoft ebay myspa facebook Linked in Cumble 2	ora whisper WIKIPEDI
twitter YAHOO AO Alibaba com	slideshare
FOURSQUARE Pinterest yelp You	tripadvisor flick
Bai amazon.com _ snapchat	Andex Preddit

## 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?

- 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





## 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

- 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



## **P9: Missing or Insufficient Session Expiration**

## How to check?

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

## How to boost?

- Configure to automatically logout after X hours / days or user-defined WEB.C
- 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)

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



# 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: <u>https://www.owasp.org/index.php/OWASP Top 10 Privacy</u> <u>Risks Project</u>

 $\rightarrow$  Feel free to contribute

- Internet Privacy Engineering Network (IPEN): <u>https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/IPEN</u>
- Project sponsor: <u>http://www.msg-systems.com</u>
- My personal blog: <u>http://securitybydesign.de/</u>



