

The Privacy Flag Observatory: A Guide to GDPR Privacy Friendly Technologies

Dr. Vasileios Vlachos
Assistant Professor

Department of Computer Science and Engineering
University of Applied Sciences of Thessaly / TEI of Thessaly
vsvlachos@gmail.com



**PRIVACY
FLAG**



Co-funded by the
European Union



Co-funded by the
Swiss Confederation

Privacy Flag Project Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployments



PRIVACY FLAG

About the Speaker



- Assistant Professor. Department of CS. University of Applied Sciences of Thessaly
- Senior Researcher. Research Academic Computer Technology Institute (RA CTI - intrinsically affiliated with the University of Patras Department of Computer Engineering and Informatics)
- Member of the Board of Directors Hellenic Association of Computer Engineers (HACE) - Technical Chamber of Greece (TEE)
- Member of the Board of Directors Greek Free and Open Source Software (GFOSS)
- Member of the Board of Directors Greek Computer Society (GCS)
- ISACA Bronze Member
- Associate Member of the Institution of Electronic & Electrical Engineers (IEEE)
- Deputy Coordinator of the OWASP Greek Chapter
- Also invited speaker in most important Greek IT Conferences
- Invited speaker or / and trainer in many workshop, seminars for Armed Forces and Law Enforcement Agencies in Greece and SE Europe







Co-funded by the
European Union



Co-funded by the
Swiss Confederation



About CTI

-  One of the major R&D institutes in Greece
-  Has undertaken more than 85 R&D projects
-  The team involved in Privacy Flag works within CTI's Research Unit 1 (RU1) which consists of 7 Faculty Members, 9 PhD Researchers and 20 Engineers-PhD Students
-  The CTI team is involved in relevant FP7 and national projects in the privacy/security, crowdsensing / crowdsourcing and IoT (PROTOS, ABC4Trust, IoT Lab)



Co-funded by the
European Union



Co-funded by the
Swiss Confederation



PRIVACY FLAG

What happened in 25th of May?



Co-funded by the
European Union



Co-funded by the
Swiss Confederation



PRIVACY FLAG

What is the GDPR?



PrivacyFlag AddOn User

Third party tracker or advertising company



Cookies

Fingerprinting

Traffic analysis



Co-funded by the
European Union



Co-funded by the
Swiss Confederation



PRIVACY FLAG

Why is GDPR important?



“DATA IS THE NEW GOLD”



Neelie Kroes
Vice-President of the European
Commission and European
Commissioner for Digital Agenda



Co-funded by the
European Union

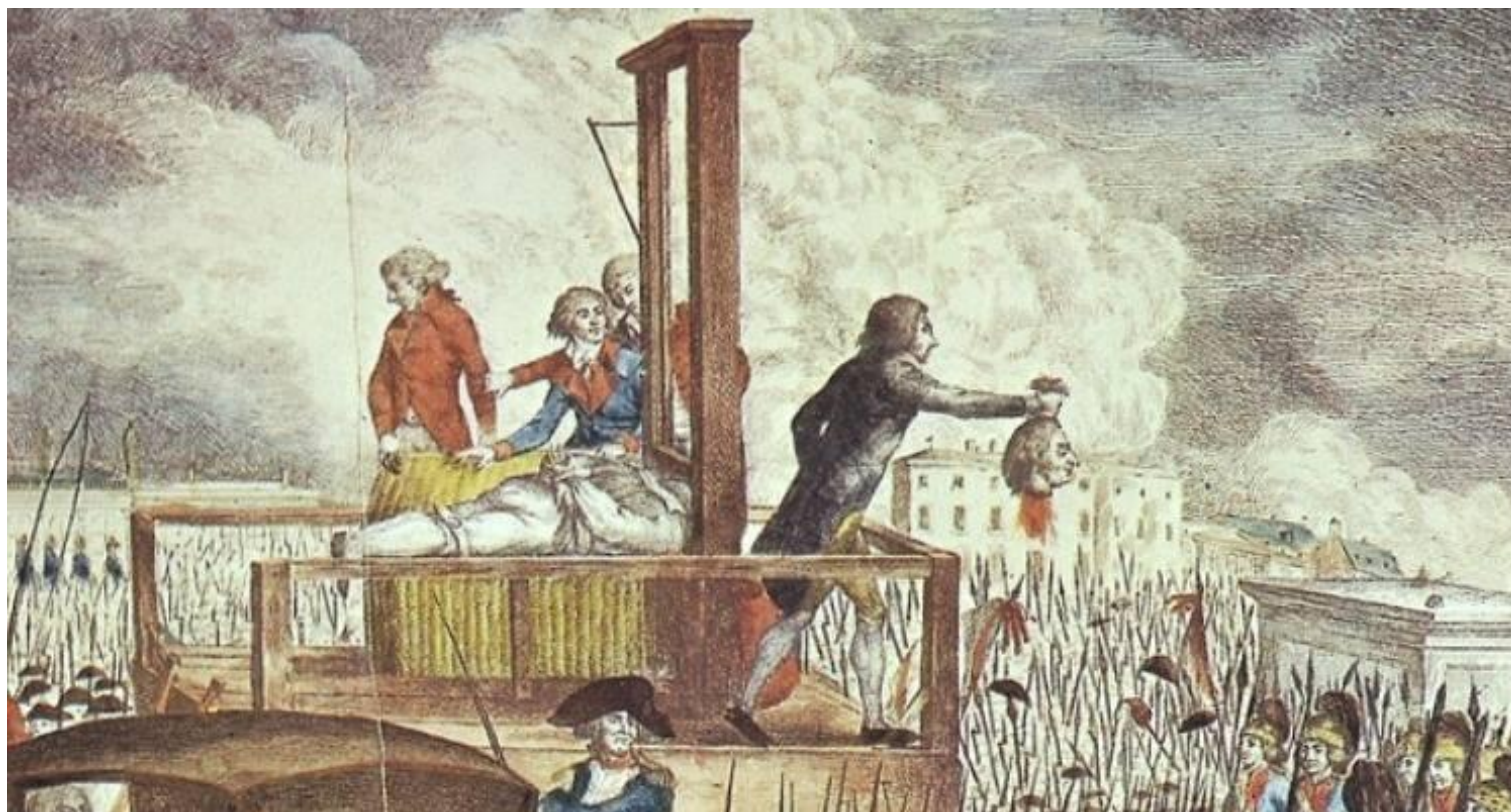


Co-funded by the
Swiss Confederation



PRIVACY FLAG

Why is GDPR important?



Co-funded by the
European Union



Co-funded by the
Swiss Confederation

Avoid the so-called experts

For the selection of GDPR partners,
firstly be informed about:

- How many years of experience have they in the field of IT Security?
- What projects have they implemented?
- With which companies / organizations have cooperated?
- What's their specialization?






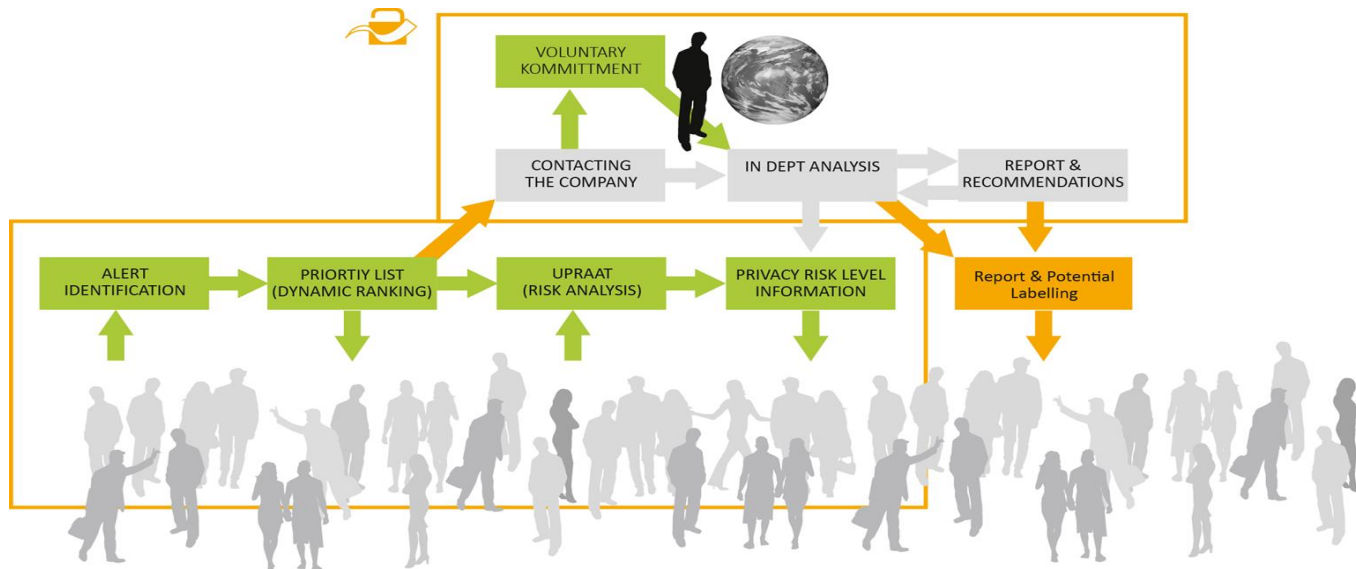
Do not hope in miracles

- The GDPR is a process, not a product
- Compliance is gradual, not steep
- You cannot buy it, only implement it.
- It's not against but in favor of businesses



Privacy Challenges

-  None of the above solutions provides a holistic approach (web, mobile, IoT)
-  Techno-legal challenges
-  Technical vs Human solution





PRIVACY FLAG



National and Kapodistrian
University of Athens



The PrivacyFlag Project

MAIN GOALS OF THE PROJECT



Privacy Flag is developing a highly scalable privacy monitoring and protection solution with:

- Crowdsourcing mechanisms to identify, monitor and assess privacy-related risks;
- Privacy monitoring agents to identify suspicious activities and applications;
- Universal Privacy Risk Area Assessment Tool and methodology tailored on European norms on personal data protection;
- Personal Data Valuation mechanism;
- Privacy enablers against traffic monitoring and finger printing;
- User friendly interface informing on the privacy risks when using an application or website.



Privacy Flag is building a global knowledge database of identified privacy risks, together with online services to support companies and other stakeholders in becoming privacy-friendly, including:

- In-depth privacy risk analytical tool and services;
- Voluntary legally binding mechanism for companies located outside Europe to align with and abide to European standards in terms of personal data protection;
- Services for companies interested in being privacy friendly;
- Researching the potential for standardization, labelling and certification.



Privacy Flag will work in close interaction with standardization bodies and will actively disseminate towards the public and specialized communities, such as ICT lawyers, policy makers and academics.

11 European partners, including SMEs and a large telco operator, bring their complementary technical, legal, societal and business expertise; strong links with standardization bodies and international fora; and outcomes from over 20 related research projects. It intends to pave the way to a privacy defenders community.

News

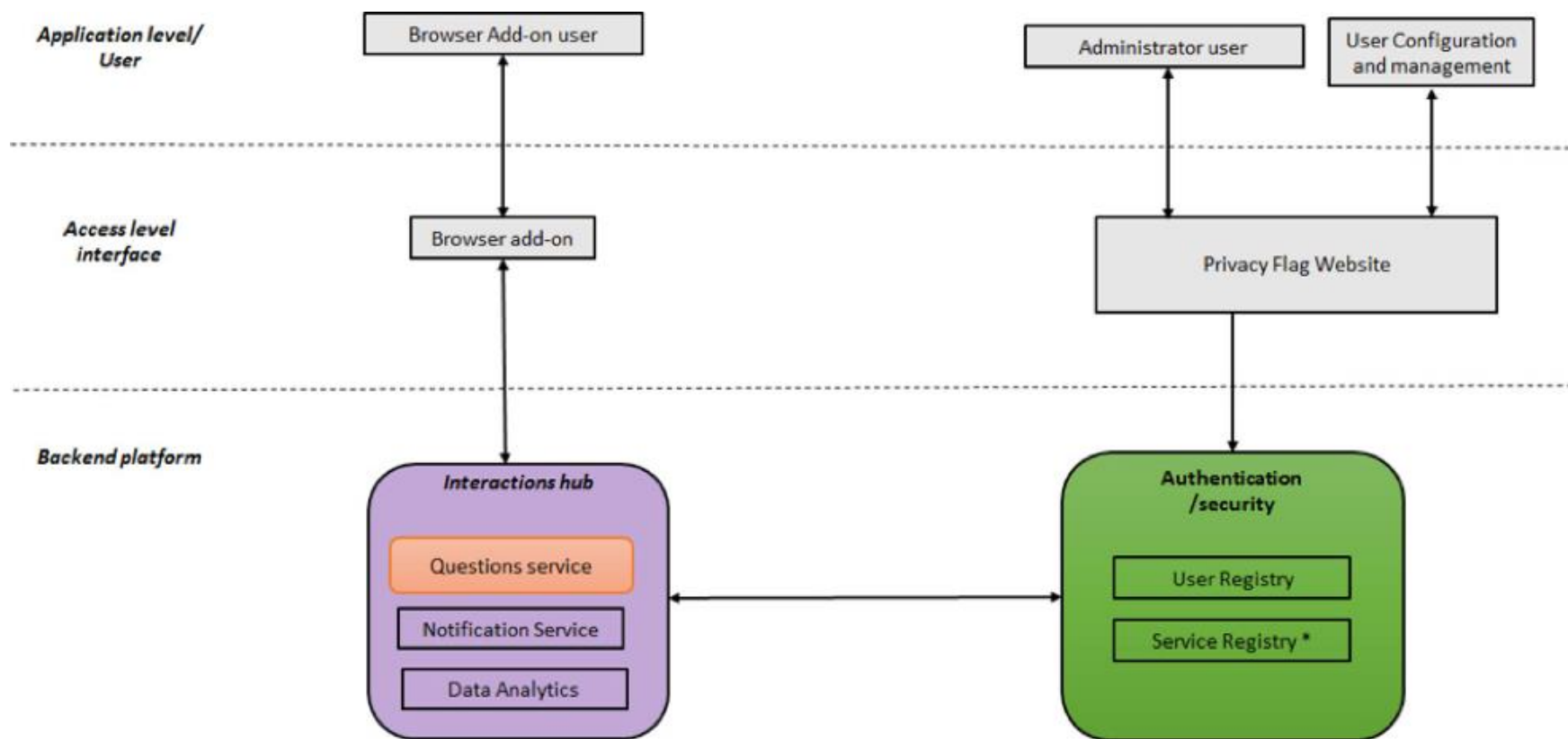


Co-funded by the
European Union



Co-funded by the
Swiss Confederation

The Privacy Flag Project - Contextual View

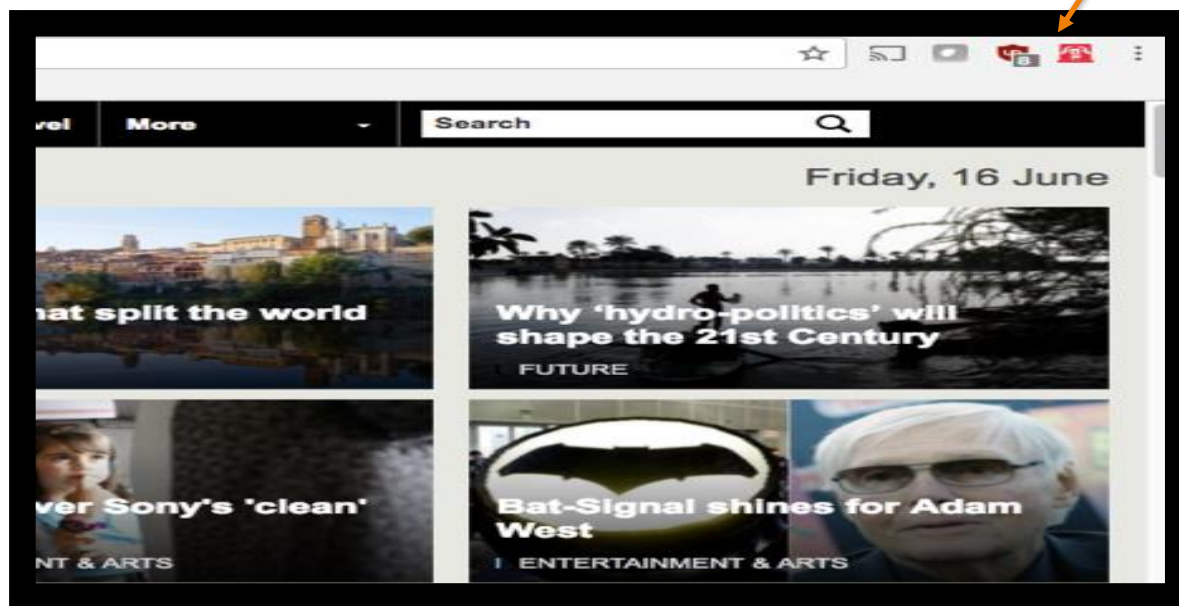




The Privacy Flag Extension

Step 1: user browses through the internet

PF flag quickly shows the evaluation of the site



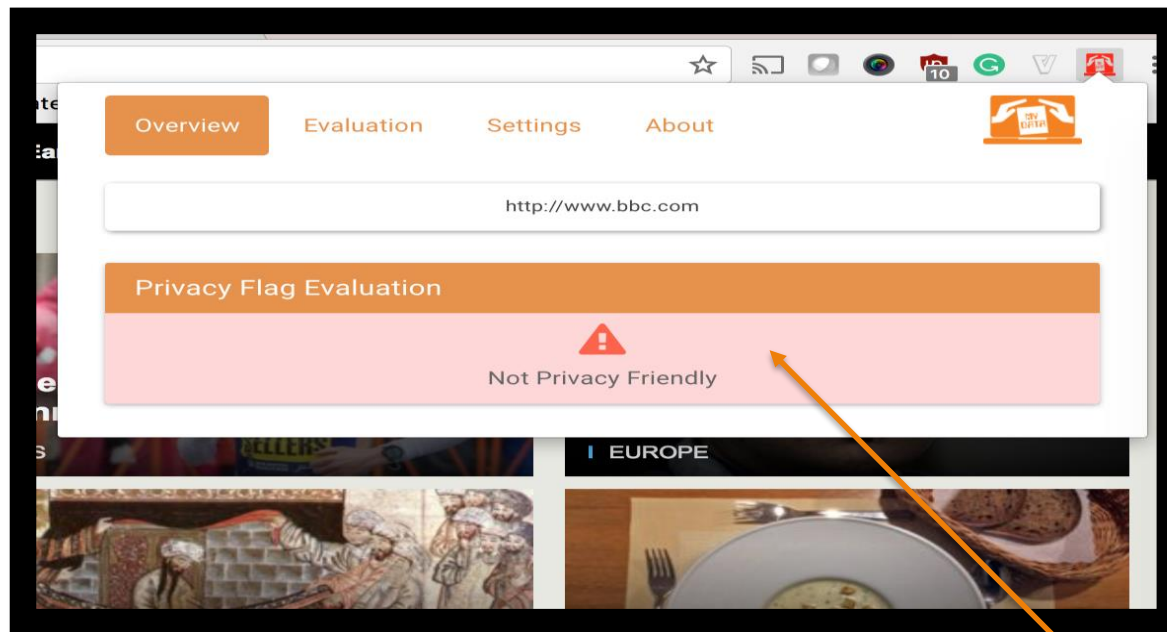
Co-funded by the
European Union



Co-funded by the
Swiss Confederation

The Privacy Flag Extension

Step 2: user opens the add-on to view more info



Current Evaluation



The Privacy Flag Extension

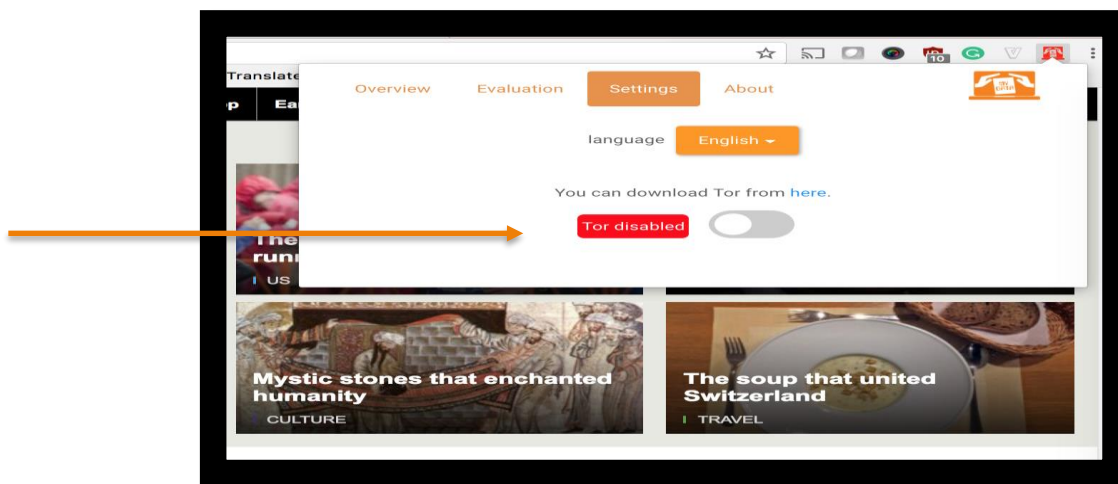
Step 3: user provides his own evaluation

User submits his evaluation



The Privacy Flag Extension

Optional Steps: Users can enable or disable ToR network functionality to improve their privacy protection



Co-funded by the
European Union

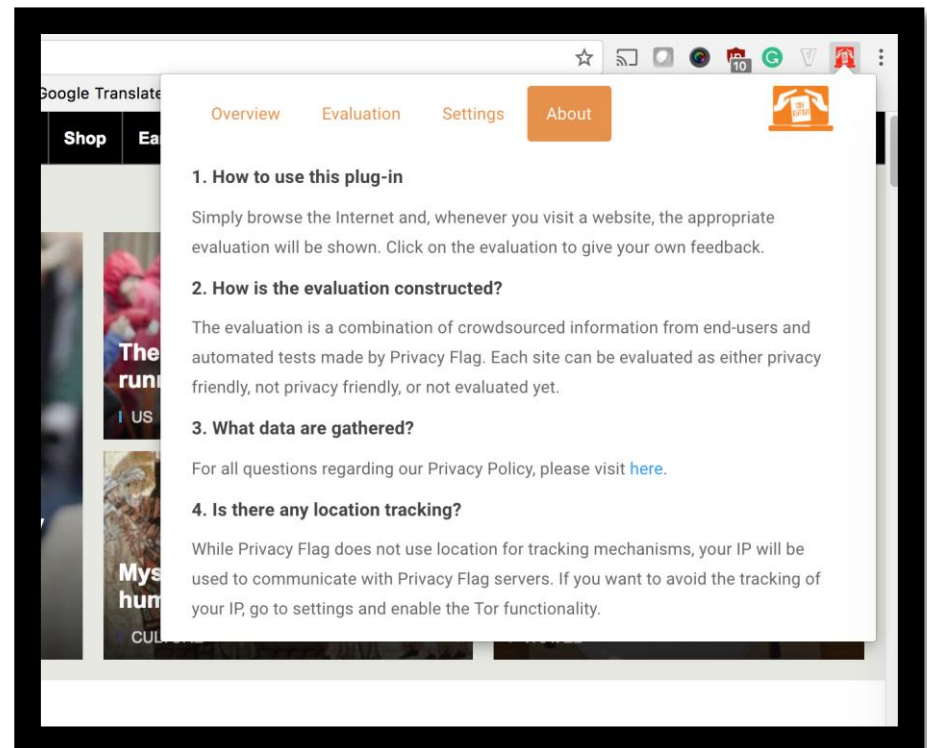
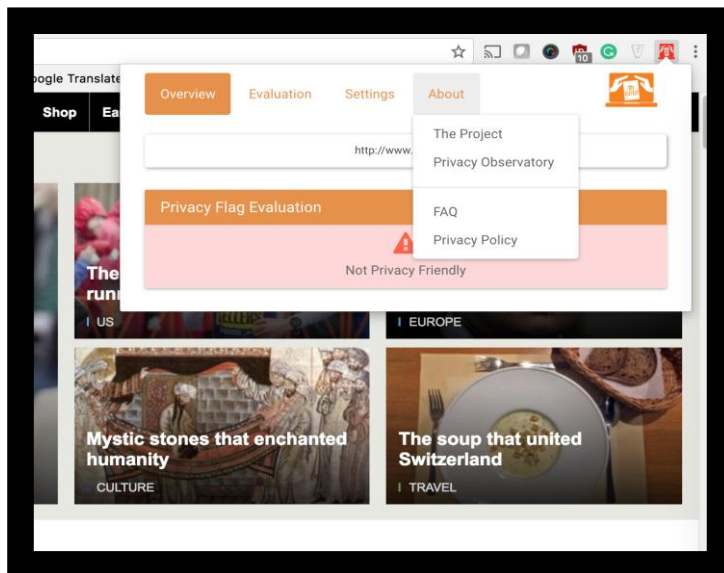


Co-funded by the
Swiss Confederation



The Privacy Flag Extension

Information Steps: users can navigate to a small FAQ section for more information or click the links to the project, PF observatory and privacy policy






Co-funded by the
European Union



Co-funded by the
Swiss Confederation



The Privacy Flag SmartApp

-  A tool to inform users on privacy risks from the applications installed in his mobile (Android)
-  A tool to inform users on privacy risks from IoT networks in the area (or across globe)
-  Characterize an app or IoT network as “privacy friendly” or “not privacy friendly” based on
 - ❖ User evaluation (URPAAM)
 - ❖ Automated threat recognition (Distributed agents – based on Android permissions – used only for apps)






Co-funded by the
European Union

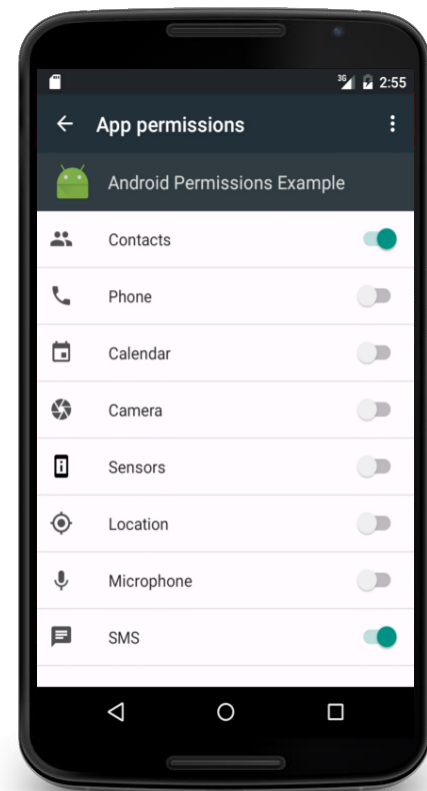


Co-funded by the
Swiss Confederation



Android Dangerous Permissions & Permission Groups

-  Introduced in Android 6.0 (API level 23), October 2015
-  "data or resources that involve the user's private information, or could potentially affect the user's stored data or the operation of other apps"
-  When apps need dangerous permissions, user has to explicitly grant the permission to the app





Android Dangerous Permissions & Permission Groups

Permission Group	Permission	Permission Group	Permission
CALENDAR	Read Calendar Write Calendar	PHONE	Read Phone State Call Phone Read Call Log Write Call Log Add Voicemail Use Sip Process Outgoing Calls
CAMERA	Camera		Body Sensors
CONTACTS	Read Contacts Write Contacts Get Account Name		Send Sms Receive Sms Read Sms Receive Wap Push Receive Mms
LOCATION	Access Fine Location Access Coarse Location		
MICROPHONE	Record Audio	STORAGE	Read External Storage Write External Storage



Allow Android
Permissions Example
to access your
location?

DENY

ALLOW



Co-funded by the
European Union



Co-funded by the
Swiss Confederation



The Privacy Flag SmartApp



Co-funded by the
European Union



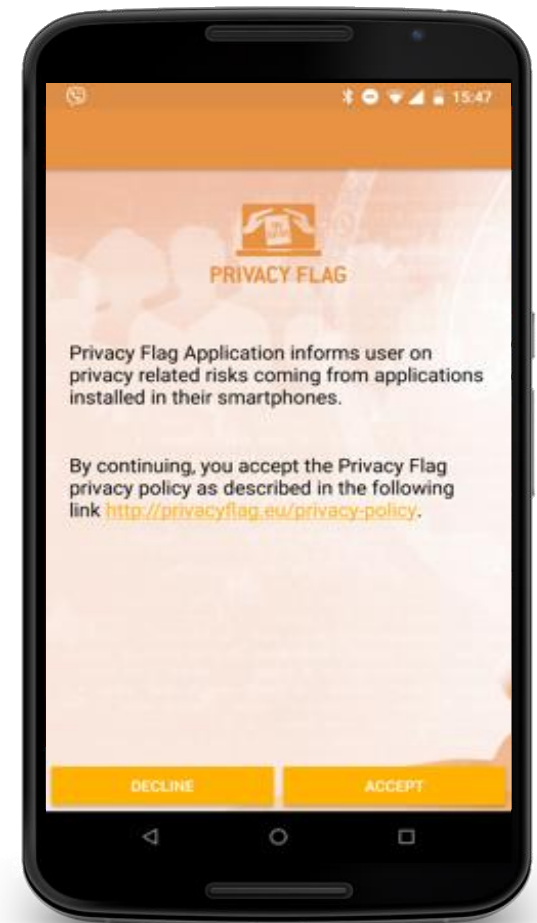
Co-funded by the
Swiss Confederation



The Privacy Flag SmartApp

Step 1: Users opens the app for the first time

User is asked to accept the Privacy Flag Privacy Policy. Declining closes the app. If the user accepts, he will not be asked again.



Co-funded by the
European Union

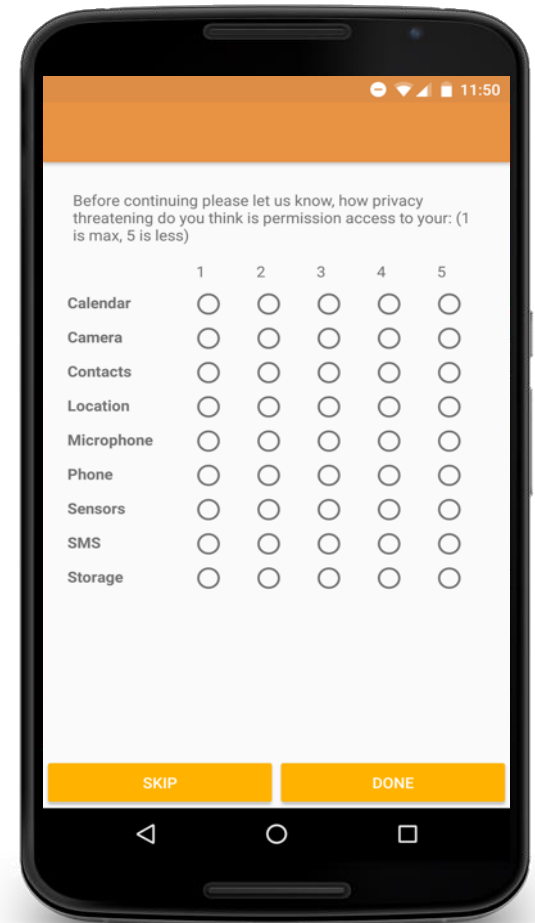


Co-funded by the
Swiss Confederation

The Privacy Flag SmartApp

Step 2: User preferences (optional – only once)

- User is asked to classify the 9 main Android permission categories, how threatening each one is, according to his/her opinion.
- As long the user is not responding this questionnaire, it will be shown every time he/she opens the app.



Before continuing please let us know, how privacy threatening do you think is permission access to your: (1 is max, 5 is less)

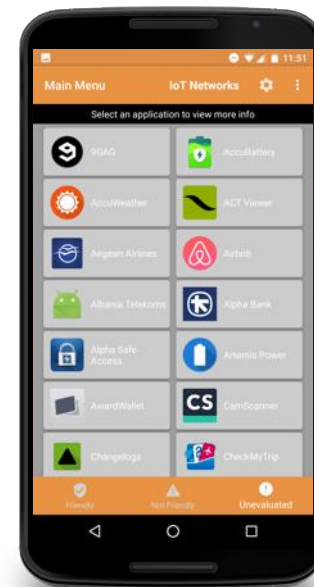
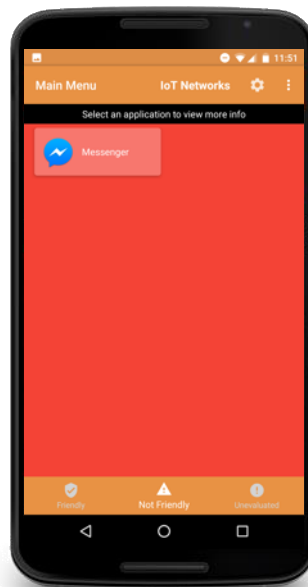
	1	2	3	4	5
Calendar	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Camera	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Contacts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Location	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Microphone	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Phone	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Sensors	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
SMS	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Storage	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

SKIP DONE



The Privacy Flag SmartApp

Step 3: User can navigate through the screen and view installed applications based on their existing evaluation



Co-funded by the
European Union

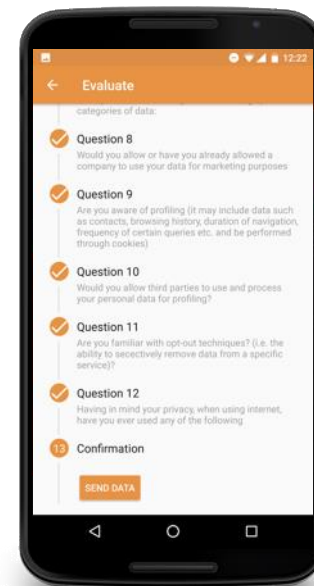
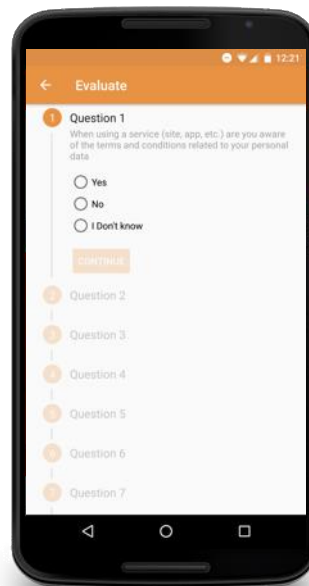
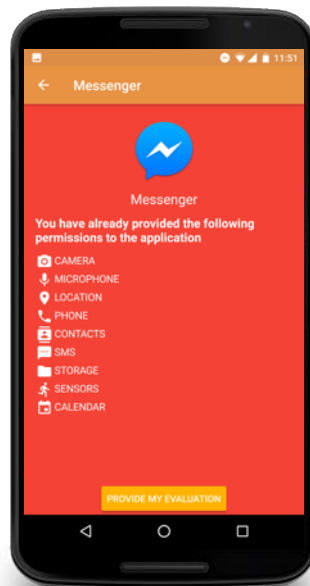


Co-funded by the
Swiss Confederation



The Privacy Flag SmartApp

Step 4: For each application, user can view more information as the permissions given and provide his/her evaluation



Co-funded by the
European Union

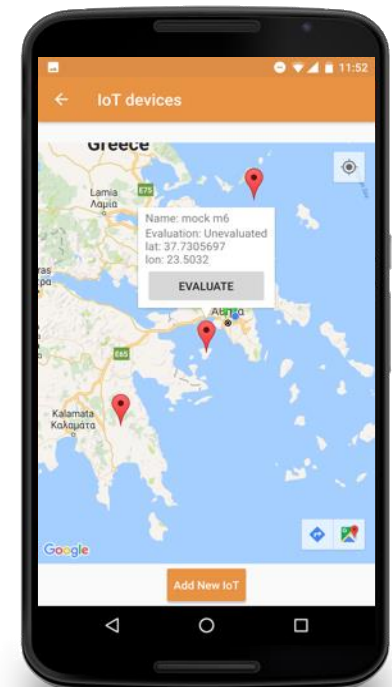
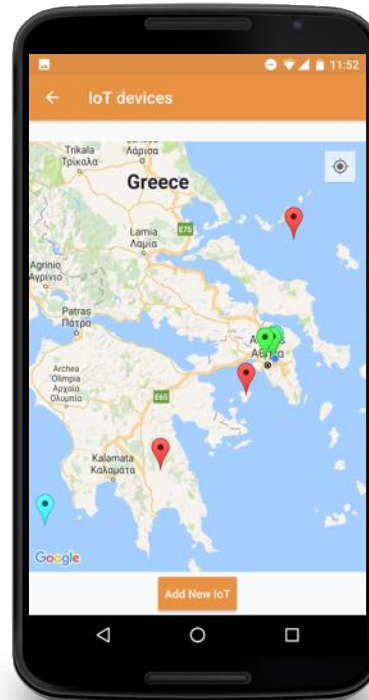
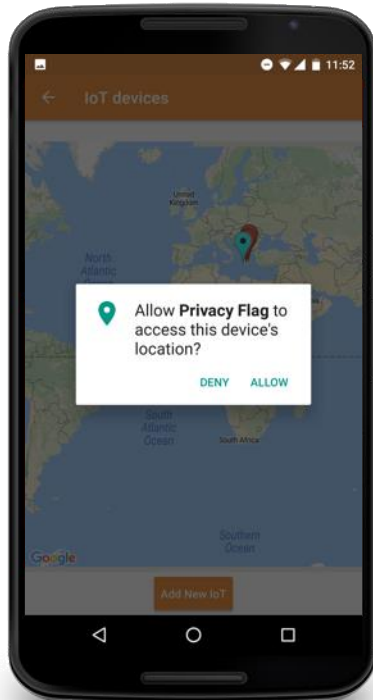


Co-funded by the
Swiss Confederation



The Privacy Flag SmartApp

Step 5: By selecting IoT networks the user can view the existing IoT networks in a map view. (optional) If the user accepts to use his/her location, the map will focus around the phone region



Co-funded by the
European Union

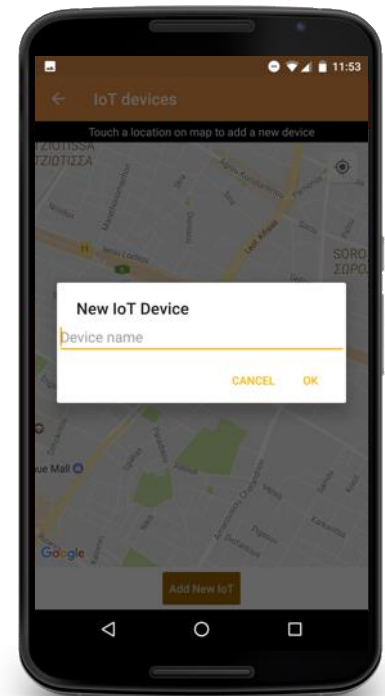
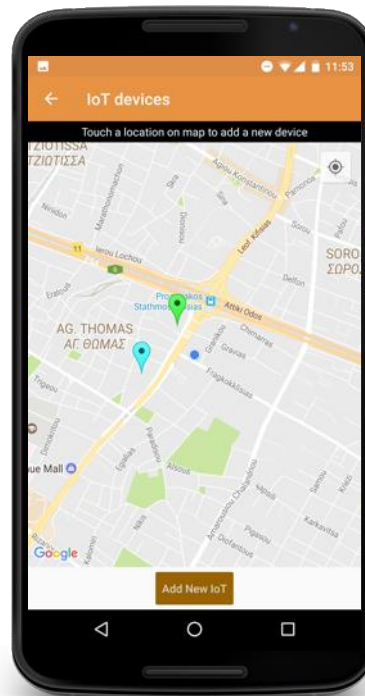
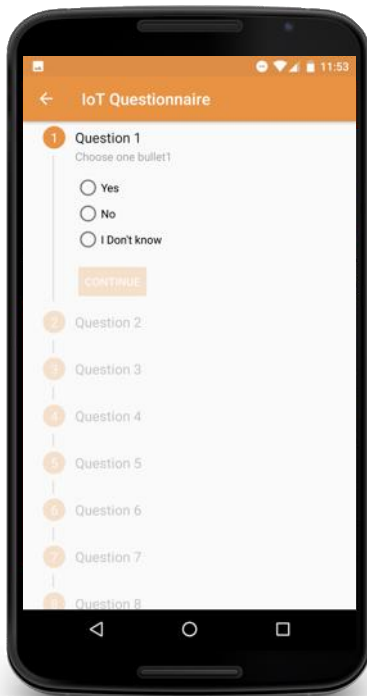


Co-funded by the
Swiss Confederation



The Privacy Flag SmartApp

Step 6: User has the ability to evaluate an IoT network through UPRAMM or by dropping a pin to add a new one.



Co-funded by the
European Union



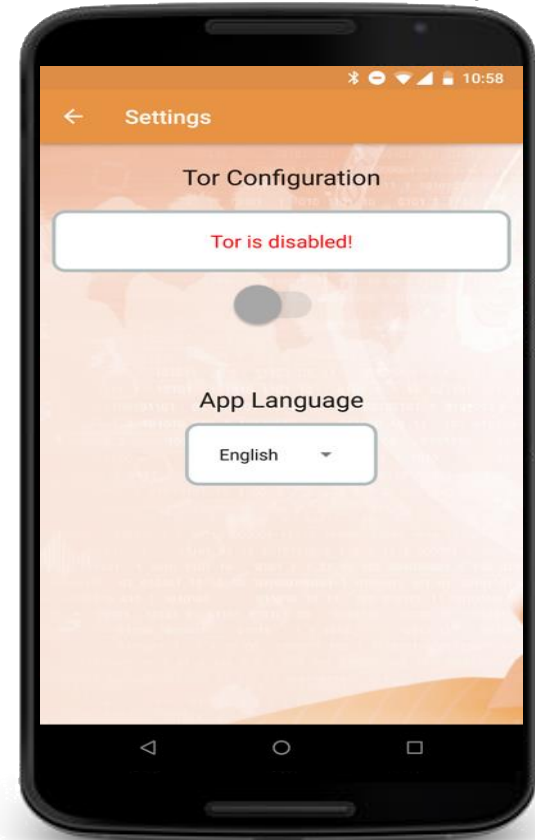
Co-funded by the
Swiss Confederation



The Privacy Flag SmartApp

Step 7 (optional): User can optionally enable or disable Tor functionality

Tor will allow the user to use the application with the maximum possible anonymization



Co-funded by the
European Union



Co-funded by the
Swiss Confederation

Privacy Flag Observatory Index

Evaluation Algorithm designed and implemented to evaluate the websites through the PF addon and the installed applications through the PF Smartphone App.

The scoring system is based on:

- UPRAAM Score
- Technical Score of the devices

The Total Evaluation is estimated as follows:

Technical Analysis Types	WebAddON	SmartPhoneApp	IoTPlatform
UPRAAM/Technical Analysis	Green	Orange	Red
Green	Green	Orange	Red
Orange	Orange	Orange	Red
Red	Red	Red	Red

Privacy Flag Observatory Index

Website and application final assessment:

A simple rule of two-thirds majority (the 66% rule) is used to generate evaluations with a minimum level of consensus when users provide contradicting evaluations.

66 %rule	Flag	Evaluation
Green > 66%	Green	Privacy Friendly
Orange > 66 %	Orange	Privacy Issues
Red > 66%	Red	Privacy Unfriendly
otherwise	Grey	Undecided



Privacy Flag Technical Score

New algorithm for technical analysis of the Web Addon was implemented, based on **boolean automatic checks** on various threats.

Expected return values

	Threat Name	
1	Does the website provide data encryption (SSL/TLS)?	True
2	Does the website provide HSTS?	True
3	Is backward compatibility with insecure SSL or TLS versions disabled?	True
4	Does the website use a trustworthy certification chain?	True
5	Does the website use Certificate pinning?	True
6	Does the website comply with any known privacy policy eTrust, P3P, published privacy policy?	True
7	Is SDNS enabled?	True

	Threat Name	
8	Does the website use technologies with known security issues - Flash?	False
9	Does the website use potentially dangerous advanced HTML5 APIs: Web Audio API?	False
10	Does the website use potentially dangerous advanced HTML5 APIs: WebRTC?	False
11	Does the website use potentially dangerous advanced HTML5 APIs: Geolocation (GPS)?	False
12	Does the website use technologies with known security issues - ActiveX?	False
13	Does the website use technologies with known security issues - Java?	False
14	Does the website use technologies with known security issues - Silverlight?	False
15	Does the website use technologies with known security issues - PDF?	False

Score	Output
11 - 15 points	Green
6 - 10 points	Orange
0 - 5 points	Red

The final technical score is estimated as:



PRIVACY FLAG

Privacy Flag SmartApp Technical Score

New algorithm for technical analysis of the smartphone app was implemented, based on **the android dangerous permission groups**.

Permission Groups	Minor/Major	Score
'android.permission-group.CAMERA'	major	2
'android.permission-group.CALENDAR'	minor	1
'android.permission-group.MICROPHONE'	major	2
'android.permission-group.CONTACTS'	major	2
'android.permission-group.LOCATION'	major	2
'android.permission-group.STORAGE'	major	2
'android.permission-group.PHONE'	major	2
'android.permission-group.SMS'	major	2
'android.permission-group.SENSORS'	minor	1
	Max Score	16

Score	Output
0 - 6 points	Green
7 - 10 points	Orange
11 - 16 points	Red

The final technical score is estimated as:



Co-funded by the
European Union



Co-funded by the
Swiss Confederation



PRIVACY FLAG

Privacy Flag Threat Observatory

Privacy Flag

Threat Observatory / Early Warning System

The PrivacyFlag Observatory is focused to provide a holistic overview of the privacy landscape in the modern Internet. The basic idea is to inform users, developers, stakeholders and researchers on the level of adoption of best practices as well as how prevalent are insecure, obsolete and deprecated technologies. Furthermore, interested parties can observe the rate of commitment in privacy related technologies for the most important web sites, since PrivacyFlag is based on crowdsourcing.

PrivacyFlag Observatory is organized in three distinct categories, Confidentiality, Security and Privacy of Data. All of them are related to the Privacy of your Data in direct or indirect way. Find why:



Co-funded by the
European Union



Co-funded by the
Swiss Confederation



PRIVACY FLAG

Privacy Flag Threat Observatory

Confidentiality

Security

Privacy

Confidentiality

Confidentiality means to ensure that unauthorized access to information is not permitted and that accidental disclosure of sensitive information is not possible. Common confidentiality controls are user IDs, passwords and encryption. Data encryption is the basic mechanism to protect the confidentiality of your information to remain private. It is absolutely necessary to encrypt sensitive data as passwords, credit card number etc but it is even better to encrypt everything. Modern web sites provide various encryption mechanisms. In PrivacyFlag we check whether a website respects users privacy by encrypting his/her data. The following information helps you to made aware of common confidentiality mechanisms next time you visit a website!



Co-funded by the
European Union

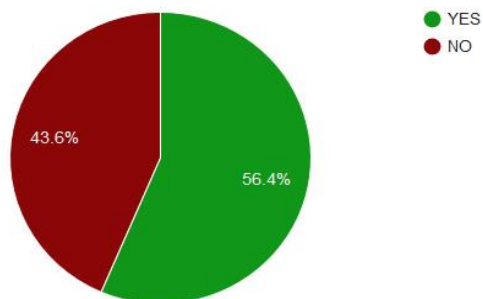


Co-funded by the
Swiss Confederation

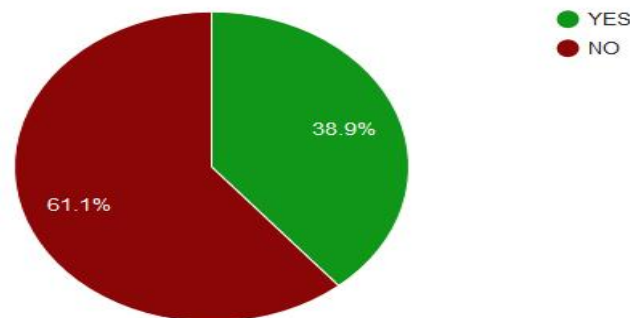


Privacy Flag Threat Observatory

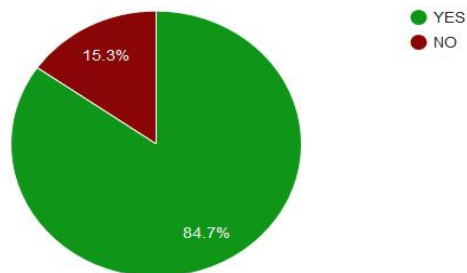
Percentage of websites that provide data encryption (SSL/TLS).



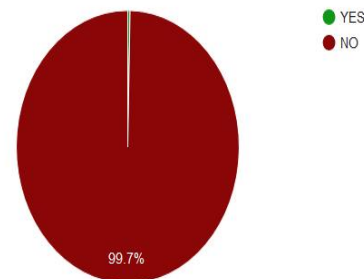
Percentage of websites that provide HSTS.



Percentage of websites that use a trustworthy certification chain.



Public Key Pinning: Experimental feature for additional security installations.



Co-funded by the
European Union



Co-funded by the
Swiss Confederation



PRIVACY FLAG

Privacy Flag Threat Observatory

Confidentiality

Security

Privacy

Security

In Internet nothing can be 100% secure. On the other hand, there are some technologies that are less secure than others. Usually, more prone to security defects are either obsolete and deprecated solutions that are no longer up to modern standards or new untested solutions that despite good design intentions do not meet always all the requirements. Nonetheless, some of these technologies are quite prevalent but they should be used with caution.



Co-funded by the
European Union



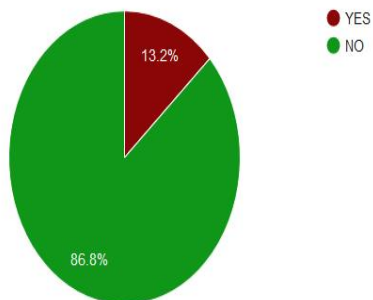
Co-funded by the
Swiss Confederation



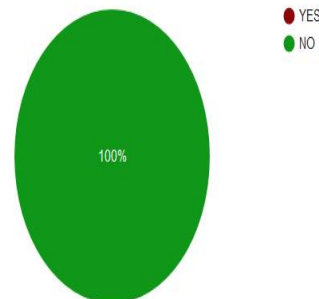
PRIVACY FLAG

Privacy Flag Threat Observatory

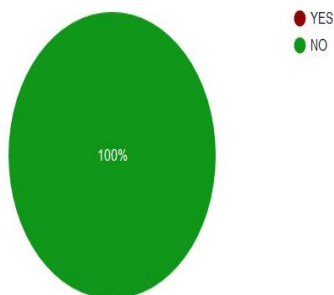
Percentage of websites that use Flash, a technology with known security issues



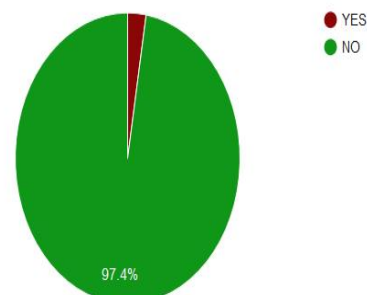
Percentage of websites that use potentially dangerous advanced HTML5 APIs - Web Audio API.



Percentage of websites that use potentially dangerous advanced HTML5 APIs - WebRTC.



Percentage of websites that use technologies with known security issues - ActiveX.



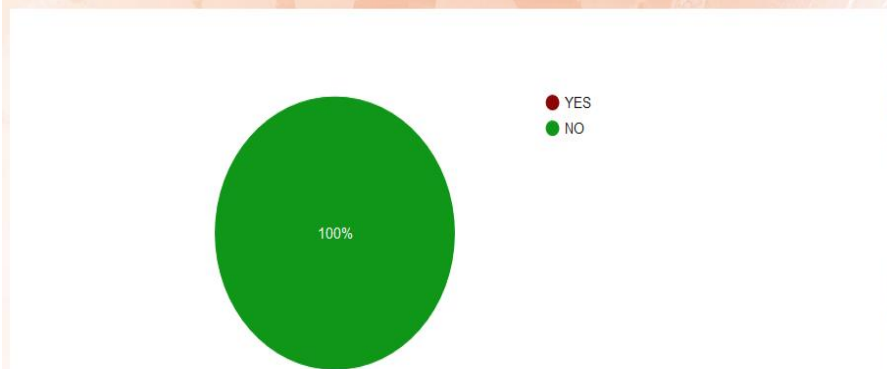
Co-funded by the
European Union



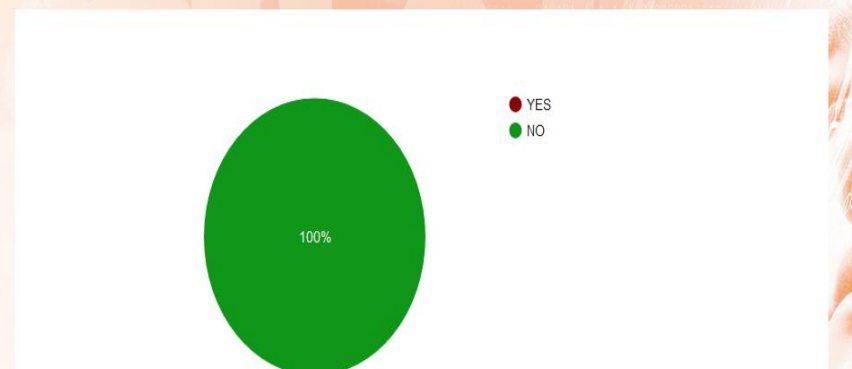
Co-funded by the
Swiss Confederation

Privacy Flag Threat Observatory

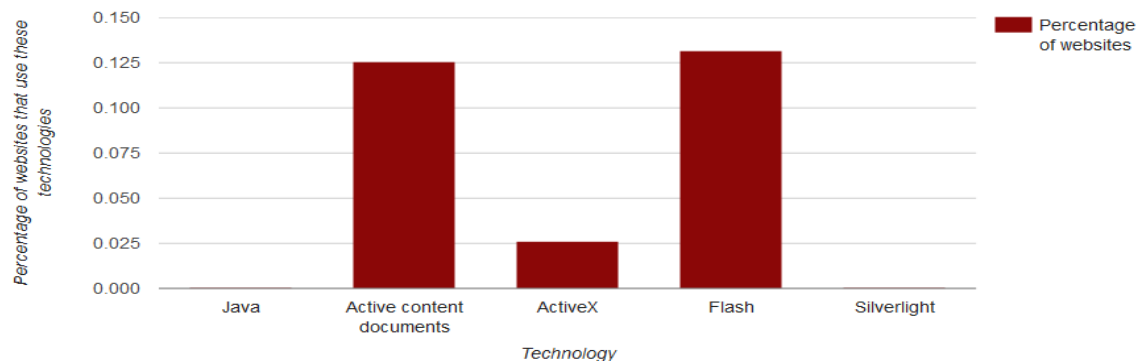
Percentage of websites that use technologies with known security issues - Java.



Percentage of websites that use technologies with known security issues - Silverlight.



Percentage of websites that use technologies with known security issues.





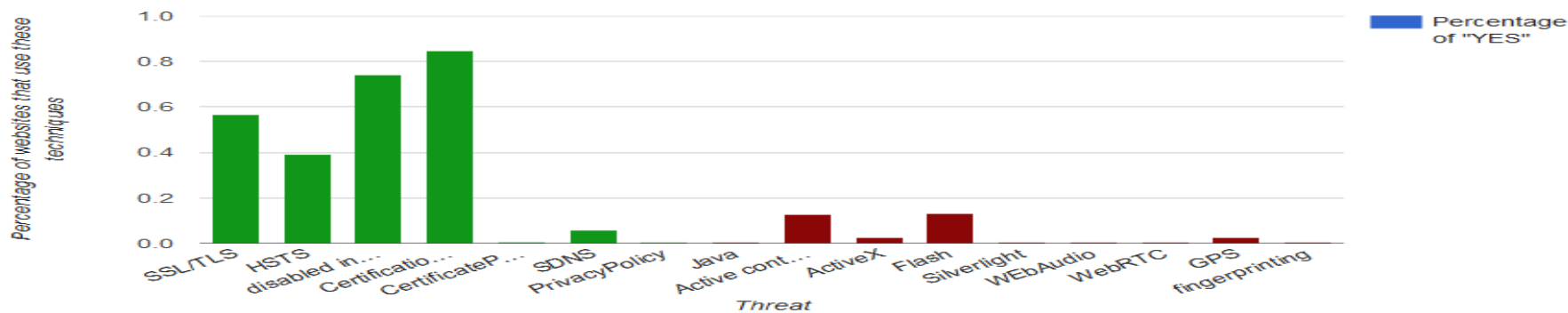
PRIVACY FLAG

Privacy Flag Threat Observatory

Percentage of websites that use potentially dangerous advanced HTML5 APIs.



Percentage of websites that use following techniques.



Co-funded by the
European Union



Co-funded by the
Swiss Confederation



PRIVACY FLAG

Privacy Flag Threat Observatory

Confidentiality

Security

Privacy

Apps' Permissions

Apps' Permissions

Each android application is associated with a list of permissions that it requires to have access and all permissions are organized into groups. There is a list of permissions that are considered dangerous. PF analyzes the permissions and permission groups that each installed application has and evaluates them accordingly.



Co-funded by the
European Union



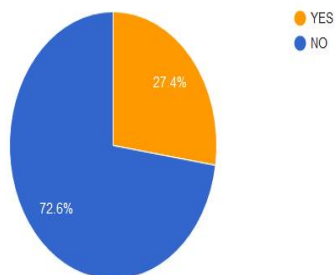
Co-funded by the
Swiss Confederation



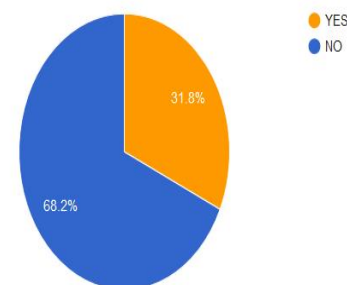
PRIVACY FLAG

Privacy Flag Threat Observatory

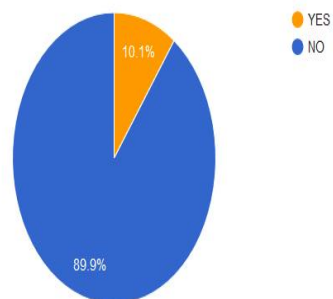
Percentage of evaluated apps that use permissions that belong to Camera group



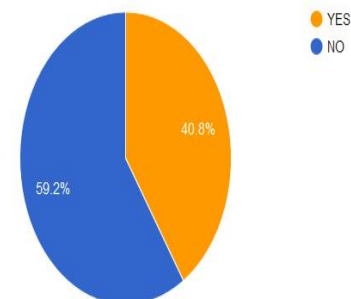
Percentage of evaluated apps that use permissions that belong to Contacts group



Percentage of evaluated apps that use permissions that belong to Calendar group



Percentage of evaluated apps that use permissions that belong to Location group



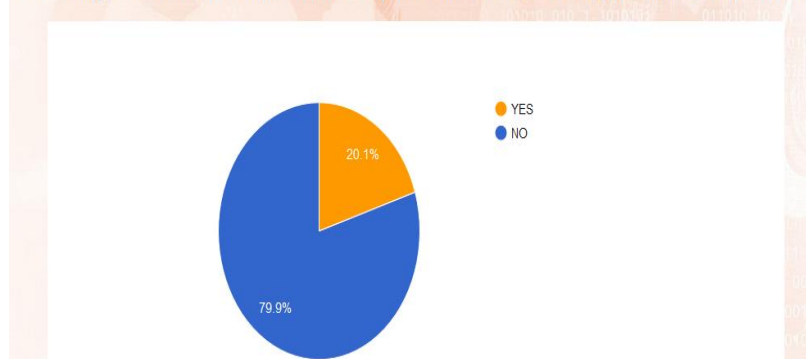
Co-funded by the
European Union



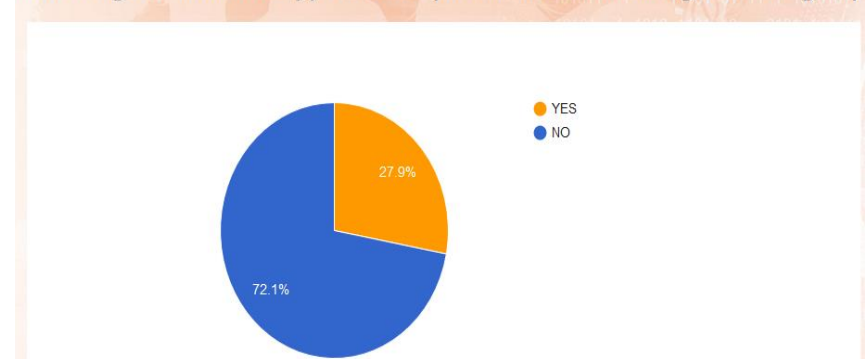
Co-funded by the
Swiss Confederation

Privacy Flag Threat Observatory

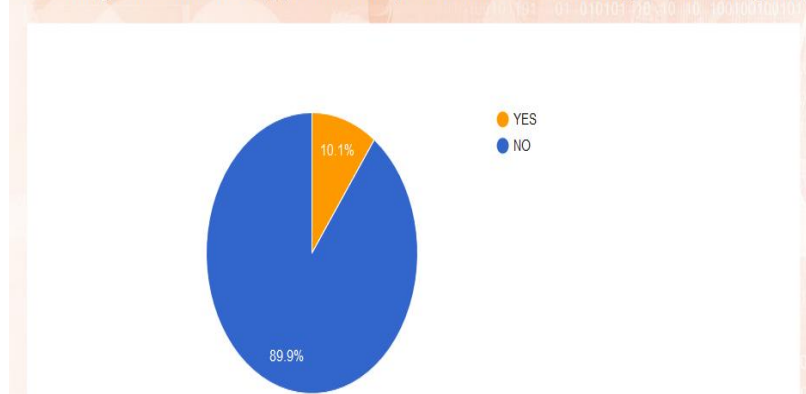
Percentage of evaluated apps that use permissions that belong to Microphone group



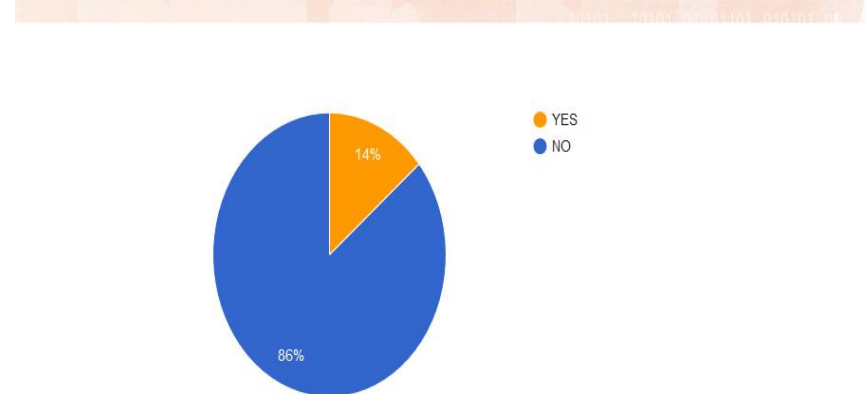
Percentage of evaluated apps that use permissions that belong to Phone group



Percentage of evaluated apps that use permissions that belong to Sensors group.

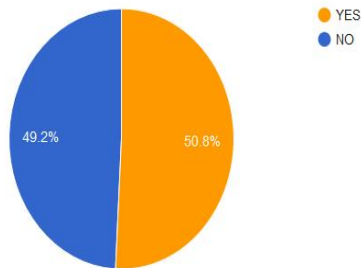


Percentage of evaluated apps that use permissions that belong to SMS group.

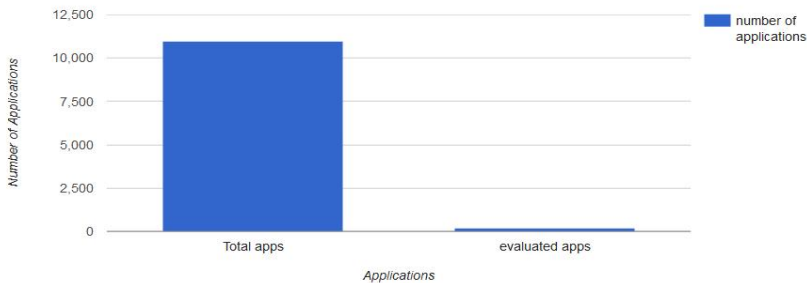


Privacy Flag Threat Observatory

Percentage of evaluated apps that use permissions that belong to Storage group

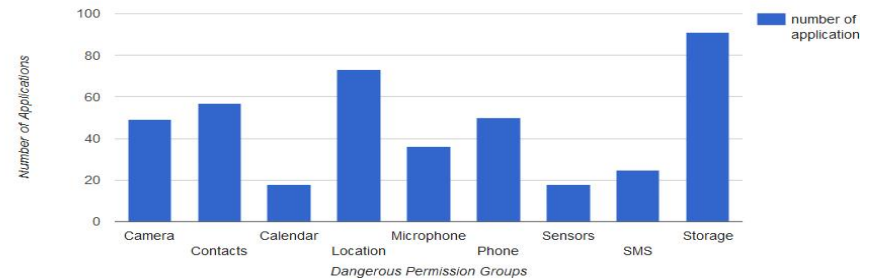


Number of apps in users' devices and number of evaluated apps by users.



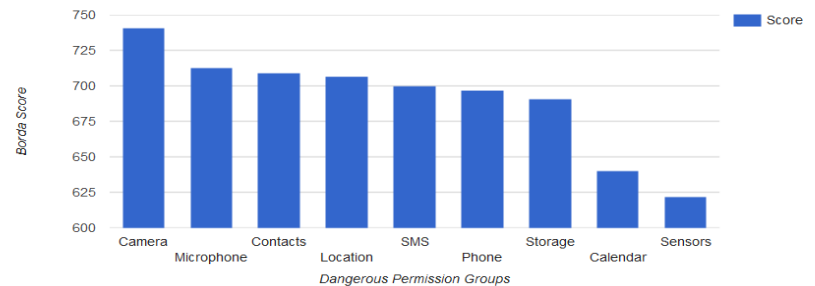
The PF Smartphone App stores in PF database all installed applications on user devices. However, the number of applications that are evaluated by the users is lower since users have to select to evaluate each application.

Number of evaluated apps that have permissions in each dangerous group



This graph depicts the actual number of the evaluated applications that have permissions in each dangerous permission group.

User Preferences.

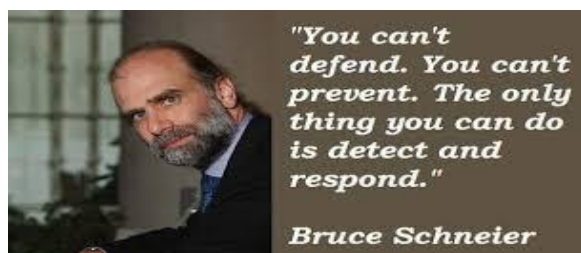
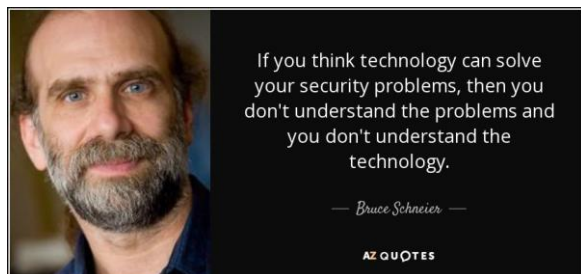


The PF Smartphone App stores user preferences regarding the dangerous permission groups. This graph depicts an ordering of them (from most dangerous to the least one) which is estimated using [Borda Count](#).



PRIVACY FLAG

Conclusions



Co-funded by the
European Union



Co-funded by the
Swiss Confederation