

## Privacy Flag: An Approach to support Privacy in Modern Communications

#### Dr. Ioannis Chochliouros – OTE Head of Research programs Section, Fixed

Infocom World 2016 \_ Athens, Greece, Nov.02, 2016 Privacy Flag- based Special Session







Co-funded by the Swiss Confederation

Privacy Flag Project Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployments - GA No.653426



**Conceptual Position** 

#### **Enabling Crowd-sourcing based privacy protection** *for smartphone applications, websites and Internet of Things (IoT) deployments.*









101011 1 11101 01 11 1 101010 10101 1 1010 1101 10 0101 1 101 01-010101 10 10 10 10010010010 1010 010 1-1010101 011010 10 10101 10101 010101 010101 00

#### Co-funded by the European Union



Infocom World 2016 \_ Athens, Greece, Nov.02, 2016 Privacy Flag - based Special Session

### **Project General Description**



### **General Information**

- Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things' deployments.

- European Research Project under the H2020 Framework Programme

- Digital Security Call: Cybersecurity, Privacy & Trust, H2020-DS-2014-1







101011 1 11101 01 11 1 101010 10101 1 1010 1101 10 0101 1 1 101 01-010101 10 10 10 10010010010 1010 010 1-1010101 01 011010 10 10101 10101 010101 010101 00

**Overview and Objectives** 

#### Co-funded by the European Union





### **Overview**

#### WHAT

 Research and combination of the potential of crowdsourcing, ICT technologies and legal expertise to protect citizens' privacy when visiting websites, using smartphone applications or living in a smart city.



Web browser

add-on

HOW

Smartphone app.

- Enable citizens to monitor and control their privacy.
  Provide user friendly tools for smart phone and web browsers enabling citizens to easily identify the level of privacy risk.
- **Build a global knowledge database on privacy risks** related to websites, smart phone applications, and smart cities.
- Raise awareness of other stakeholders, providing a positive incentive to privacy friendly companies and services versus privacy-unfriendly ones.









**Objectives\_(1)** 

- 1. Develop a highly scalable privacy monitoring and protection solution based on:
- Crowd sourcing mechanisms to identify, monitor and assess privacy-related risks.
- Privacy monitoring agents distributed on users' smart phones and web browsers, to identify privacy threatening activities and applications.
- Universal Privacy Risk Area Assessment Tool and methodology tailored on European and international legal norms on personal data protection and data ownership;
- Personal Data Valuation mechanism for citizens;
- **Privacy enablers for citizens to retain control over their privacy** with optimized anonymisation techniques against traffic monitoring and finger printing;
- User friendly interface informing the users and raising citizen awareness on their privacy risks when using a smart phone application or visiting a website







### **Objectives\_(2)**

- 2. Develop a global knowledge database of identified privacy risks with websites, smart phone applications and smart cities deployments, together with on-line 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 of Europe to align with and abide to European standards in terms of personal data protection.
- Services for companies interested in being privacy-friendly.
- Labelling and certification process and service.







### **Objectives\_(3)**

**3. Collaborate with standardization bodies** (such as *ISO, ETSI, ITU* and *IEC*) and actively disseminate towards the public and specialized communities, including ICT lawyers, policy makers and academics.

 Privacy Flag will develop a privacy defenders community and will establish a legal entity with a sound business plan

to ensure a long term exploitation, sustainability and maintenance of the Privacy Flag platform and services.











Co-funded by the Swiss Confederation



### **Architecture and Processes**







### **Architecture and Processes**



Co-funded by the European Union





101011 1 1101 01 11 1 101010 10101 1 1010 1101 10 0101 1 101 01-010101 10 10 10 10010010010 1010 010 1-1010101 011010 10 10101 10101 010101 010101 00

## Co-funded by the European Union



Infocom World 2016 \_ Athens, Greece, Nov.02, 2016 Privacy Flag - based Special Session

### **Key Technical Development**





#### Main Privacy Flag platform (Crowdsourcing-based privacy risk analysis)

End-users	Risk focus	Evaluators	User interface	Tools	Data storage	Related tasks
CROWD	Websites	CROWD	Browser	Add-on + security agent	Common Knowledge Database	T4.3, T4.2
	Smartphone applications		Smartphone	Apps + security agent		T4.4, T4.2
	loT deployments		Website	Web page		T4.6

Complementary tools (indepth analysis)

End-users	Risk focus	Evaluators	User interface	Tools	Data	Related tasks
Solution provider	ICT Solution	Experts	Website	Indepth analytisis tool	Database	T6.4, T3.3
provider						







**Universal Privacy Risk Area Assessment Methodology** Universal & Generic Reliable & Effective Democratizing Privacy Legal & **Technical Requirements** 

UPRAAM









### **IoT Deployments**



### Websites

Apps

OB



**PRIVACY FLAG** 



Co-funded by the Swiss Confederation









### In-depth analysis

-111











Main Components







### Main Components\_(1)

**Privacy monitoring agent:** software to be deployed on users' devices for monitoring and detecting suspicious application or website behaviour.

- It will perform a local check on sensitive functions and data transmissions in order to inform the enduser on identified risks and level of risk.
- It will inform the user about any identified risk and may share information on suspicious applications or websites with the common knowledge database.
- Any information transfer will be full anonymized and will exclude and filter out any personal data.

## **Privacy enablers** ensuring that the user of the platform cannot be identified -or tracked- when connecting to the platform or to other web services.

 Inter-alia, it will ensure that transmitted data can be fully secured and anonymized, addressing among others IP and MAC tracking (through translation and proxy mechanisms), as well as unwanted GPS location transmission.

# **Privacy Risk Alert tool** enabling any user to launch an alert on any suspicious application, website or unusual deployment of IoT devices in a smart city that could constitute a risk on privacy.

The list of alert will be made available to the crowd for risk evaluation process by volunteers and/or experts. This alert tool will enable to rank and prioritize the applications according to the users priority concerns.







### Main Components\_(2)

### Universal Privacy Risk Area Assessment Tools & Methodology

(UPRAAM) will be designed and made available to the crowd, in order to enable the crowd to "assess the risk" on their privacy related to websites, smartphones applications and Internet of Things deployments in smart City.

- It will translate complex norms into a user friendly evaluation tool to be used by the public at large and accessible to non-specialist.
- A complementary UPRAAM version will be designed for researchers in order for them to "self-assess" the privacy risks related to their planed experiment.
- UPRAAM will also serve as a basis for the in-depth evaluation tool to be performed by experts as a paying service for interested companies.

#### **Privacy Risk Flag add-on for browsers** to be inserted by the user in his/her Internet browser.

- It will include the privacy monitoring agent as well as a connection to the common knowledge database in order to alert the user on the level of privacy risk attached to the website he/she is accessing. The information will appear as a graphical symbol next to the navigating tool of the browser.
- It will also give a direct access to the UPRAAM and additional Privacy Flag resources, and will serve to invite the crowd to assess suspicious websites according to the UPRAAM.







Main Components\_(3)

#### **Privacy Risk Flag application for smart phone** will be developed for Android environment, with potential extension to other operating systems.

- The Privacy Flag smart phone application will include the privacy monitoring agent as well as a connection to the common knowledge database in order to alert the user on the level of privacy risk attached to the applications he/she is using.
- It will also give a direct access to the UPRAAM, and will serve to invite the crowd to assess suspicious applications according to the UPRAAM.
- It will also provide an option to alert the user when he/she is getting physically close to an identified source of privacy risk in a city.
- It will provide a direct access to the knowledge database, evaluation tools and additional Privacy Flag resources.

## **Knowledge data base server** with the collected alerts, profiles and privacy risk level of applications and websites.

• It will be fed by the monitoring agents as well as by crowd sourcing tool and the UPRAAM and in-depth analysis results.

#### Website providing access to the tools and database on privacy risk, as

well as the backend management tool for the platform and for the in depth analytic tools.







### Links with International Standards Fora, Exploitation and Dissemination Strategy







#### PRIVACY FLAG

### Links with International Standards Fora

- **ITU-T** (MI)
- IoT Forum & AIOTI (DNET, MI)
- IPv6 Forum (UL, MI)
- ETSI (ISG IP6) (UL, OTE, MI, UoA)
- IETF, IEEE (UL, MI)
- W3C (Velti, MI)
- Digital Enlightenment Forum (CTI, MI)
- European Union Agency for Network and Information Security (ENISA) (CTI)
- Mobile Marketing Association (MMA)
- Public Safety Communication Europe
- **OWASP** (CTI)







### **Exploitation Strategy**





#### Tools - On-line assessment tool Legal entity - Smart phone app to maintain the - Browser add-on platform and Knowledge database the community Voluntary commitment tool of users **On-line resources Community of users Standard UPRAAM Methodology** Labelling





**Exploitation Plan** 

Setting up a dedicated legal entity to promote privacy

#### **Business Model**

In principle, Privacy Flag will use a dual business model:

- Free evaluation tool for the crowd: No sales revenue stream are planned on the tools developed by the project in order to enable a large adoption and to make the service freely available to the public.
- Paying services for interested companies: Privacy Flag will propose paying services for in depth privacy risk audits, recommendations and potential labelling for interested companies.

#### Competition, differentiation and competitive advantages

#### Financial projections

We plan to generate most revenues from services and consulting, with potential complementary incomes from selective advertisements. *Privacy Flag has a huge potential to be downloaded by end-users*.







### **Targeted Communication Plan**

Target group	Technical level	Main focus	Communication means	
Public / citizens	Understandable by a large public of non- specialists	Privacy Flag tools dissemination UPRAAT and personal data protection Project presentation Societal and economic benefits	Media Project website Social medias Consumers and privacy protection communities App. stores	
Research community	High level on the scientific and technical innovation and more accessible level on the legal dimension	Project presentation Scientific innovation	Conferences Publications Specialized networks/fora Project website Social medias / twits	
Legal community	High level on the legal dimension and more accessible level on the technical dimension	Legal aspects, including Privacy Risk Area Assessment Tool and voluntary binding mechanism	Conferences Publications Specialized networks/fora	
Industry, SMEs and public administrations	Focus on the technology enablers and potential business opportunity, economic exploitation and societal benefits	Project presentation Pilots opportunities Cooperation with their products and solutions Scientific and technical innovations Business opportunities Societal benefits	Direct contacts Advisory board Platforms, such as Cleanweb Initiative Conferences and fairs Publications Project website	







102011 1 11101 01 11 1 101010 20101 1 1010 1101 10 0101 1 1 101 01-010101 10 10 10 10010010010 1010 010 1 1010101 01 011010 10 10101 10101 010101 01010 00

**Project Structuring** 

#### Co-funded by the European Union







### Work Plan

- WP1 Architecture design will analyze end-user requirements to adapt and design a Privacy Flag architecture and process that will provide framework for activities in other WPs.
- WP2 Privacy risks analysis and modelling will research the privacy-related legal, technical and societal risks and design the privacy risk analytical framework.
- WP3 Assessment tools will research and develop the risk assessment tools, including the crowd-sourcing tools for risk assessment and data valuation, the in depth evaluation tools and the Voluntary compliance commitment tool.
- WP4 Technical enablers ill focus on researching and developing technical enablers, including the smartphone application, the browser add-ons and the security and privacy enablers.
- WP5 Integration, tests and validation will interconnect and integrate the various pilot buildings with the Privacy Flag platform, including the database and server implementation, the website and backend management platform, as well as end-user tests and validation.
- WP6 Outreach, dissemination and exploitation will focus on the dissemination and exploitation of the results, including the implementation of the business plan envisaged for the sustainability of the crowdsourcing platform and community.
- WP7 Coordination and management will deal with the day-to-day management of the project.







### **Expected Outcomes**

- 1. Three user-friendly and freely available tools for citizens
- 2. Distributed crowd-sourcing privacy monitoring platform
- 3. Universal Privacy Risk Area Assessment Tool & Methodology
- 4. Privacy enablers
- 5. Global knowledge database on privacy risks
- 6. Voluntary compliance commitment tool
- 7. On-line resources
- 8. In-depth privacy risk analysis on-line tool
- 9. Labelling and certification process
- **10. Standard on privacy labelling**







### Impact

- Providing an on-going platform for privacy protection Improving privacy and personal data ownership
- Improving privacy risk detection
- Improving personal data valuation
- Rebalancing the inherent asymmetry in ICT data protection
- Scalability and viral dissemination
- Designing a open standard for privacy risk analysis
- In-depth analysis, labelling and certification
- Societal impact and user awareness
- Towards a democratic model of privacy management
- Extending the geographic scope of personal data protection
- Exploring potential room for a new international convention
- User awareness

#### Economic Impact

- Rebalancing and mitigating unfair competitive advantages
- Supporting European SMEs and industry







### Links with other EU-funded projects

### IoT Lab

**PRIVACY FLAG** 

- F-Interop (MI, UL)
- TEFIS (LTU)
- Living Labs (LTU)
- ABC4Trust
- DigiTrust
- Oitisense
- SECCRIT
- SESAME
- (LTU, Velti) (CTI) (CTI) (DNET) (OTE) (OTE)

(MI, CTI)







Thank you!

### www.privacyflag.eu

#### **Dr. Ioannis P. CHOCHLIOUROS** Head of Research Programs Section, Fixed **Coordinator of the Privacy Flag Project**

Research and Development Department, Fixed & Mobile Technology Strategy & Core Network Division, Fixed & Mobile

Hellenic Telecommunications Organization S.A. (OTE) 1, Pelika & Spartis Street 15122 Maroussi-Athens,

Greece

Tel.: +30-210-6114651 Fax: +30-210-6114650 E-Mail: <u>ichochliouros@oteresearch.gr</u>; <u>ic152369@ote.gr</u>







010101 1 1 1 01000001 1011 10 1011 1 1100 01 11 1 101010 101 1 1010 1101 10 0101 1 1 11 1 01 010101 10 10 10 100100100101 10 010 1 1010101 01 010101 00 10101 10101 01 01101 010101 00

🕑 velti 🍳





uni.lu

UNIVERSITÉ DU

LUXEMBOURG

LULEÅ

OF TECHNOLOGY

UNIVERSITY,











HWCommunications Cyber Security and Resilience





Co-funded by the European Union



Co-funded by the Swiss Confederation