COSMOTE
our world is you

17th INFOCOM World Conference 2015

Athens, 24 November 2015

OTE
GROUP OF COMPANIES

Privacy Flag

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

General Info

- 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

Overview

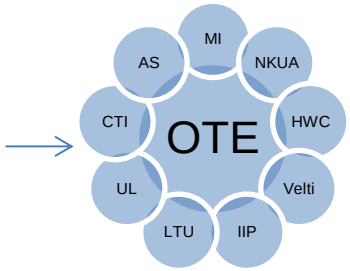
WHAT

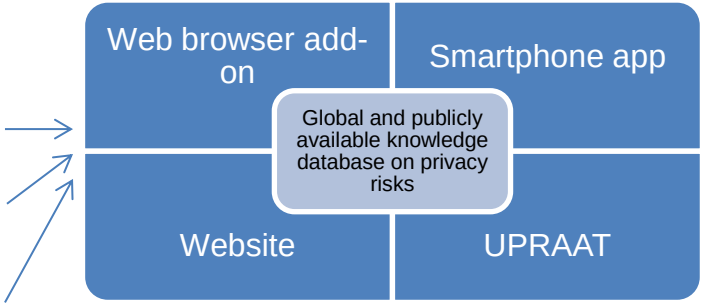
- Research and combine the potential of crowdsourcing, ICT technologies and legal expertise to protect citizens' privacy when visiting websites, using smartphone applications or living in a smart city.

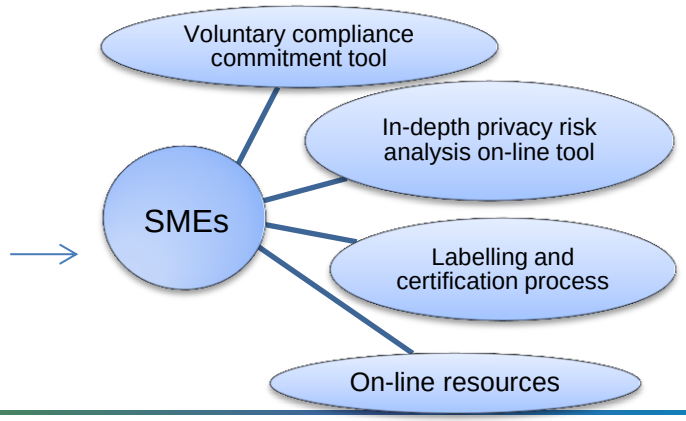
- Enable citizens to monitor and control their privacy.
- Provide user friendly tools for smart phone and web browsers enabling citizens to easily identify the level of privacy risk.
- Build a global knowledge database on privacy risks related to websites, smart phone applications, and smart cities.

- Raise awareness of other stakeholders, providing a positive incentive to privacy friendly companies and services versus privacy-unfriendly ones.

HOW







Objectives (I)

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 (II)

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 (III)

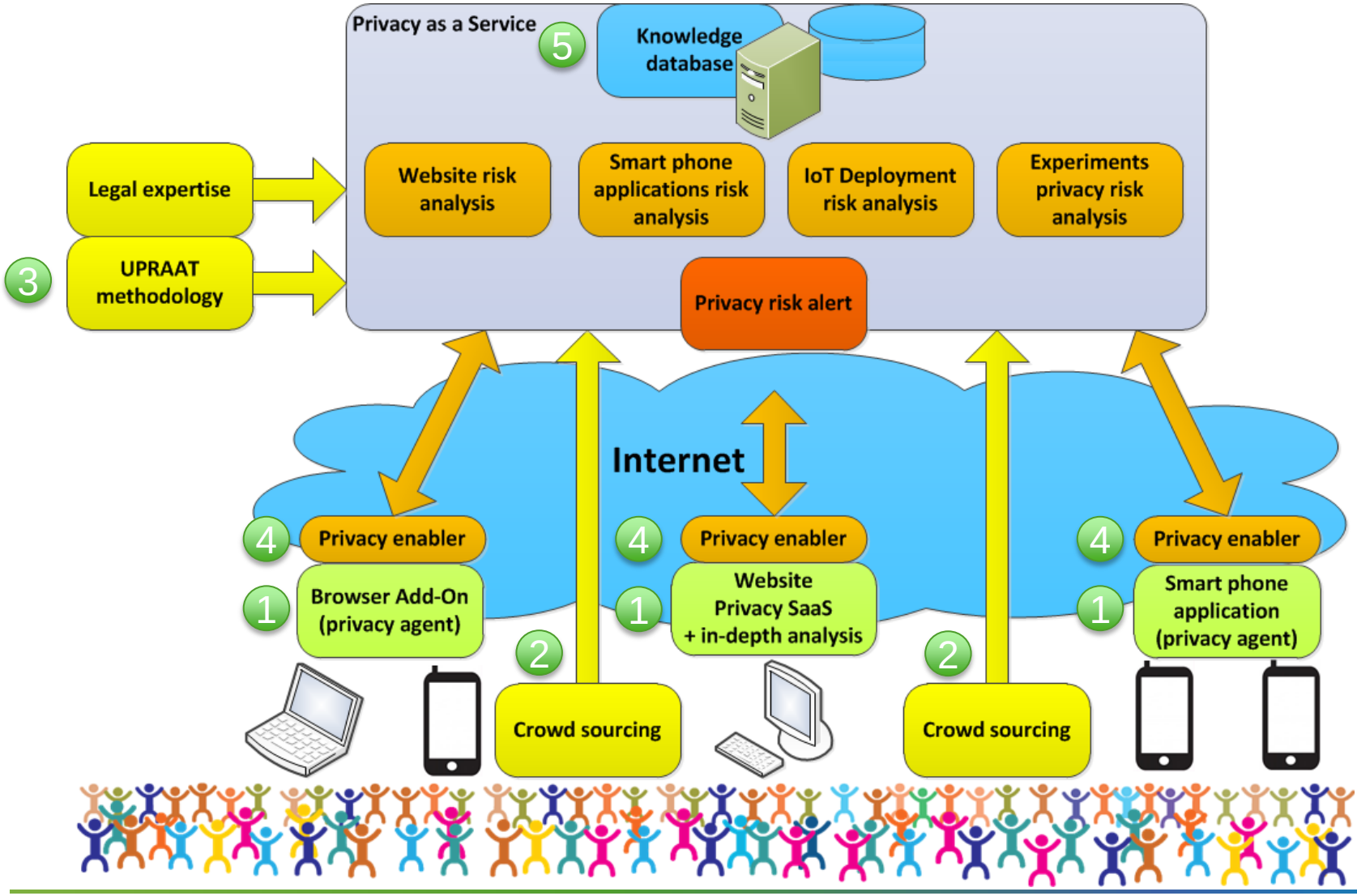
3. **Collaborate with standardization bodies** (such as ISO, ETSI, ITU, and IEC) **and actively disseminate** towards the public and specialized communities, including ICT lawyers, policy makers and academics.

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.

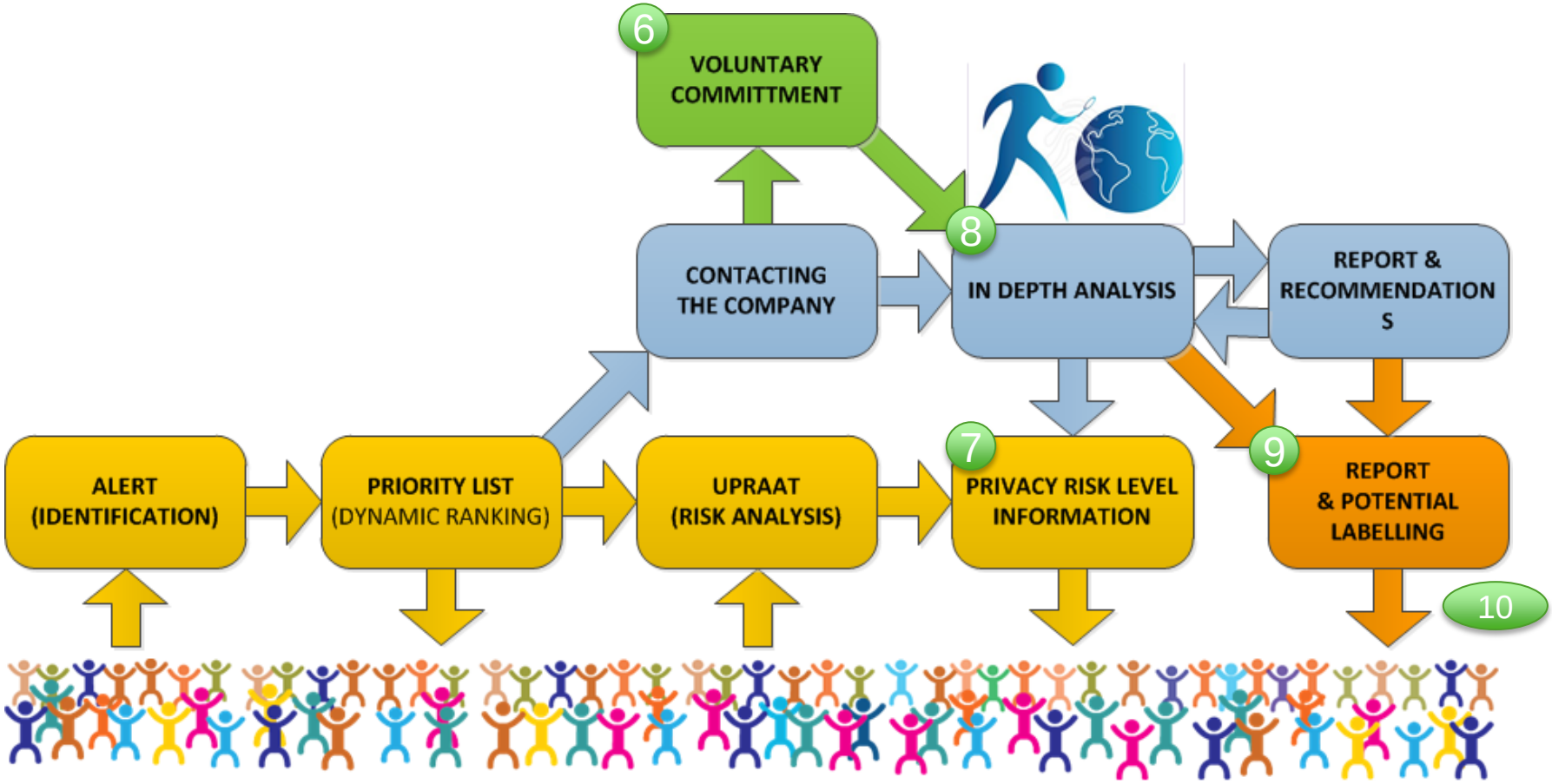
Expected Outcomes

1. Three user-friendly and freely available tools for citizens
2. Distributed crowd-sourcing privacy monitoring platform
3. Universal Privacy Risk Area Assessment Tool
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

Architecture



Process


6
VOLUNTARY COMMITTMENT
8
CONTACTING THE COMPANY
IN DEPTH ANALYSIS
REPORT & RECOMMENDATIONS
ALERT (IDENTIFICATION)
PRIORITY LIST (DYNAMIC RANKING)
UPRAAT (RISK ANALYSIS)
7
PRIVACY RISK LEVEL INFORMATION
9
REPORT & POTENTIAL LABELLING
10

Main components (I)

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 end-user 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. It will among other 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 (II)

Universal Privacy Risk Area Assessment Tools 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 UPRAAT version will be designed for researchers in order for them to self-assess the privacy risks related to their planed experiment. UPRAAT 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 UPRAAT and additional Privacy Flag resources, and will serve to invite the crowd to assess suspicious websites according to the UPRAAT.

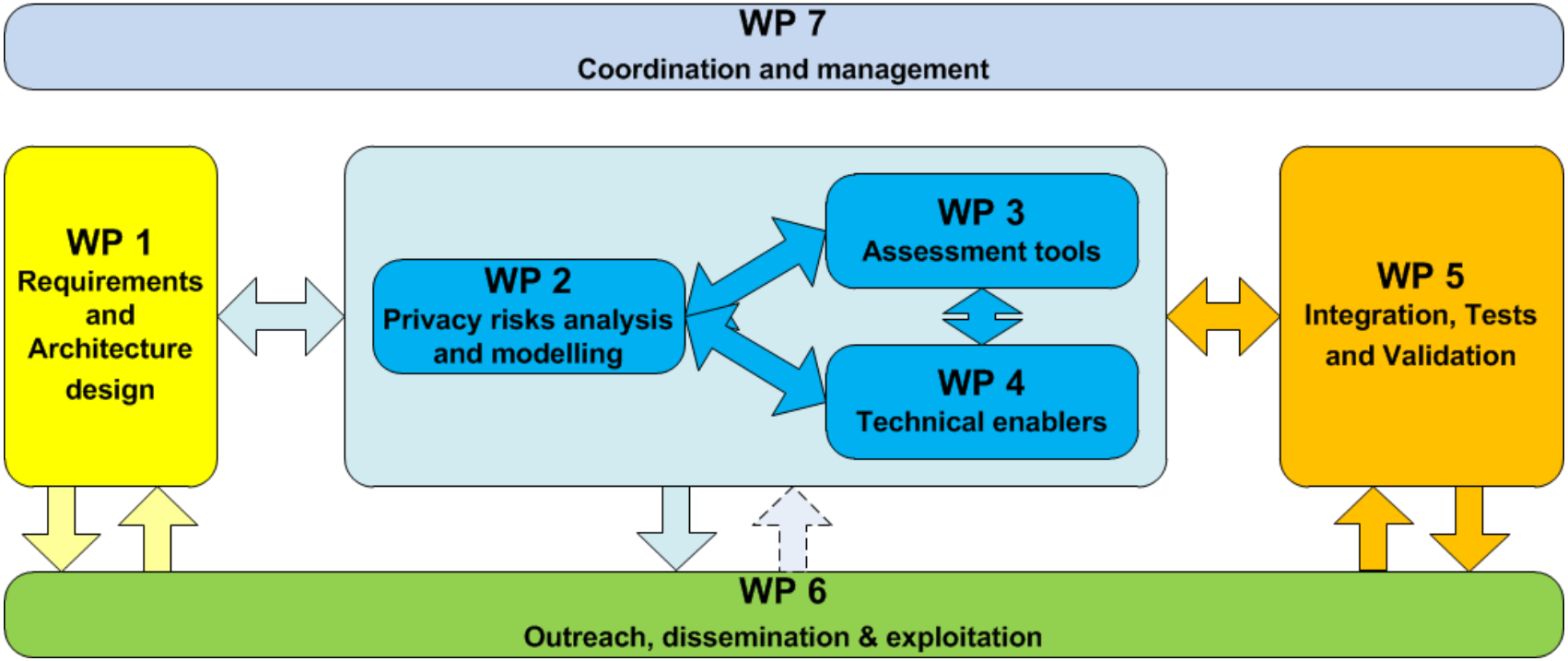
Main components (III)

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 UPRAAT, and will serve to invite the crowd to assess suspicious applications according to the UPRAAT. 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 UPRAAT 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.

WP Structure



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.

Consortium


LULEÅ UNIVERSITY OF TECHNOLOGY
MANDAT INTERNATIONAL
uni.lu UNIVERSITÉ DU LUXEMBOURG
CTI "DIOPHANTUS" computer technology institute & press
OTE
Project coordinator
Istituto Italiano per la Privacy e la Valorizzazione dei Dati
HWCommunications Cyber Security and Resilience
velti
DUNAV NET

Thank you for your attention!

For further information:

Kelly Georgiadou, Ph.D. egeorgiadou@oteresearch.gr
Maria Belesioti, M.Sc. mbelesioti@oteresearch.gr

Research Programs Section Fixed
Hellenic Telecommunications Organization S.A.
1, Pelika & Spartis str.
15122 Maroussi Athens
Greece
Tel. +30-210-6114695, +30-210-6114937
Fax. +30-210-6114650