PRIVACY: BIG BUSINESS vs. DEATH OF PRIVACY

PRIVACY FLAG PROJECT

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

I - Vision and Objectives

Personal data have become merchandisable asset encouraging various stakeholders to collect such data and trade them without the end-user awareness and acceptance. The European Union has taken the lead in adapting the legal framework to better protect the citizens' rights and interests. However, the extent of the Internet and smart phone applications, the fact that data can be retrieved without the owner knowledge and the vast majority of those applications are developed from outside the EU jurisdiction, strongly limit the possibility to effectively impose a privacy-protection framework globally with a conventional approach. Moreover, privacy norms are perceived as complex by many citizens.

The Privacy Flag project will 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. It will enable citizens to monitor and control their privacy with a user friendly solution made available as a **smart phone application**, a **web browser add-on**, and a **public website**, all connected to a shared **knowledge database**. It will benefit from the outcomes of over 18 related research projects,- in order to provide a new paradigm of privacy protection combining "endo-protection" with locally deployed privacy enablers protecting the citizens privacy from unwanted external access to their data, and "exo-protection" with a distributed and crowd-sourced monitoring framework able to provide a collective protection framework together with increased citizen awareness and implicit pressures on companies to improve their privacy compliance.

Privacy Flag will:

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 anonymization 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**

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;

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.

Our key ambition is to utilize the power of the crowd combined with ICT technology and legal expertise to enable users to monitor, control and increase their level of privacy in three targeted application domains: websites, smartphones applications, and Internet of Things deployments in smart cities. It will target different segments of end-users, including:

- Citizens, which constitute the main target group;
- Companies and SMEs;
- Smart cities and public administrations considering deploying Internet of Things;
- ICT Lawyers and policy makers.

More specifically, the Privacy Flag project aims to develop and deliver the following outcomes:

- **Three user-friendly and freely available tools for citizens**, including an Android application, an add-on for their Internet browsers and a public website. The two former ones will enable the users to monitor and identify threats on their privacy when browsing on a website or using smart phone applications. They will inform them through a user friendly interface and enable them to contribute to the crowd sourcing platform. The latter one will provide access to complementary information on privacy protection and resources, and will be accessible through the two former ones.
- **Distributed crowd-sourcing privacy monitoring platform** enabling the crowd to mutualize their efforts and resources by running a local Privacy Flag application on their smart phone and/or an add-on in their Internet browser. The application will monitor and identify privacy breaches, informing the user about the alert and uploading the information in a central database to tag the application or website as suspicious and share this information with others.

- **Universal Privacy Risk Area Assessment Tool** (UPRAAM) which will provide a clear methodology and suite of assessment tool for evaluating the level of risk on privacy and personal data protection. It will be designed in order to precisely match the European and international norms and standards related to personal data protection and privacy, while providing a simple and user-friendly interface adapted to a large audience of non-specialists. It will benefit from experts in privacy law, mobile applications and Internet of Things, including the International Association of IT lawyers, the Istituto Italiano per la Privacy, as well as experts in end-user participation and empowerment. The UPRAAM methodology will translate complex legal obligations into a user-friendly evaluation tools. It will enable the crowd to use the UPRAAM methodology through a set of user-friendly questions to objectively assess the level of risk for their privacy and to contribute to enrich a shared knowledge database.
- **Privacy enablers** integrated into the Privacy Flag application and browser add-on for privacy risk assessment and traffic analysis and protection. These tools include crowd-sourcing tools, distributed agents to monitor privacy breaches and in depth evaluation tools.
- **Global knowledge database on privacy risks** indexing websites, smart phone applications and IoT deployments, fed by the crowd (applying the UPRAAM), by alerts received from the Privacy Flag distributed monitoring agents, and by experts performing in-depth risk evaluations.
- **Voluntary compliance commitment tool** enabling any company or public administration to formally and publicly commit and abide to respect the European standards even if located outside of Europe.
- **On-line resources** to improve privacy, including legal search engine on privacy norms, templates of legal clauses for privacy friendly applications and user agreement, etc.
- **In-depth privacy risk analysis on-line tool** for experts**.** Privacy Flag will propose to SMEs and interested companies a voluntary in depth privacy risk analysis of their solutions with a report and recommendations for optimizing their practices in terms of privacy protection.
- **Labelling and certification process** will be proposed to companies and solutions which are fully compliant with the privacy requirements.
- **Standard on privacy labelling** by exploring the possibility to cooperate with the International Standards Organization (ISO), the International Electro-technic Commission (IEC) and the International Telecommunication Union (ITU) to standardize and disseminate our privacy risk evaluation methodology.

Privacy Flag gathers 11 European partners, including SMEs and a large telco operator that will ensure the alignment of the research with the market and an effective sustainable exploitation of the results. The partners combine complementary technical, legal, societal, business expertise, including in crowd sourcing, personal data protection, security, data valuation and end-user acceptance. The consortium has strong links with standardization bodies, international fora and ICT law community,- and is directly involved in over 20 related projects that will contribute to its development. Privacy Flag will set up **a legal entity** in Luxembourg to support the long term maintenance and exploitation of the platform.

By combining the UPRAAM methodology, distributed privacy monitoring agents and crowd sourcing, the platform will enable a large scale privacy risk assessment process, which would not be possible with a regular top down assessment approach. Moreover, by mutualizing the skills and capacities of the crowd, it will reverse and rebalance the asymmetric relationship between individual users in front of large and powerful companies with a clear incentive to comply with privacy protection.

II - Relation to the work programme

Privacy Flag addresses the strategic Objective of the call H2020-DS-2014-1 Digital Security: Cybersecurity, Privacy & Trust. Privacy Flag will design and develop a collective privacy protection and monitoring platform, which will integrate information various emerging technologies in such a way that end-users recover control on their privacy and data ownership rights, and application designers get incentives to comply with those rights. Privacy Flag proposes to offer a tool to support citizens to learn and participate actively in privacy protection with a highly scalable model. Privacy Flag addresses the specific challenge and scope of the call as follows:

Specific challenge	Privacy Flag contribution
ny online users are reluctant to disclose personal rmation online because of privacy concerns. **rsonal data has become an economic asset, b not the owners, i.e. the users, that control or netize it**. This is in the hands of the service viders whose business case often includes the us data they collect (e.g. social networks, search gines, online retailers, and cloud hosting services) a protection and privacy frameworks in Member tes and Associated Countries need to be lemented in a transparent and **user-friendly way p users understand how their personal data ght be used, including the economic value** of t a. Such knowledge will enable them to exercise ice and know and assert their rights. As the nomic value of their data is not known to the rage user, they are not able to evaluate the value r data relative to the value they assign to a "free" vice. Moreover, the users **have no control over at happens** with their data, e.g. they cannot verify data is not passed on to 3rd parties. This situatio y **influence individuals notion of privacy** which y be perceived as a non-valuable asset.	vacy Flag will provide user friendly tools for smart phone web browsers enabling citizens to easily identify the le isk that an application or a website will access or use th sonal data, as well as to assess the potential economic ue of their data. It will contribute to build a global wledge database on privacy risks related to websites, art phone applications, and smart cities. ill raise citizen awareness on the privacy risks and the ue of their data,- and will enable them to effectively mon control their privacy and data sharing. Moreover, by ting citizens to apply the UPRAAM methodology, it will e their understanding and awareness of personal data tection norms and standards, recognized and protected opean and international law. vacy Flag will raise awareness of other stakeholders too uding companies and public administrations and will vide a positive incentive to privacy friendly companies a vices versus privacy-unfriendly ones. ill provide technical enabler to better protect and enforc r privacy rights. In many situations it is still possible to nificantly increase the level of privacy without sacrificing usability, e.g., when applying privacy-preserving routing hniques, encrypting the data, by proving properties inste isclosing single values (e.g., proving to be at least 18y. vacy Flag will offer, depending on the scenario, adequat tection techniques to minimize the information leakage.
a protection principles need to be visibly pected for the delivery of personalised public vices, to increase trust in public administrations. **nsparency** is particularly important in an open ernment context, where personal data may be red between different departments and ninistrations or across borders and where third ties can engage in the creation and delivery of sonalised services for citizens and businesses.	vacy Flag will increase transparency and awareness over processing of personal data by public administrations by bling citizens to easily identify if personal data will be ected and by assessing the privacy risks related to smart s deployments. It will also increase the level of lerstanding of the privacy-related normative framework ulating the circulation of personal data between public ninistrations of different Member States in the European on.

Scope	Privacy Flag contribution
e focus is on the demonstration of **solutions to tect individuals' privacy by default while powering the users to set the desired level of vacy,** based on a simple to understand visualisati he privacy level, giving them control over how the a will be used by service providers (including pub horities), and making it easier for them to verify b ether their online rights are respected and if they asonable bargain.	vacy Flag will provide a simple web browser add on (to b played in the control panel of the browser as an simple ractive icon), as well as a user friendly smart phone lication, and a website. It will alert the users and block a afe website or smart phone application. It will provide a ault user warning as long as the concerned application been checked and considered as safe enough. The use be empowered to freely determine their desired level of acy requirements. finger pointing applications and web services that are aching privacy rights and sharing this information with a community of users, Privacy Flag will have a snowball ct as the community users will grow to pressure and courage such companies to respect privacy rights and to ly compensate the data owners whose data are exploite ay also increase their legal risk when breaching legal gations.
e activities may also cover **tools facilitating the ormation of individuals** about the processing of r personal data. Systems will either have to detec privacy settings automatically, or the data will ha privacy settings permanently associated to it by th r.	vacy Flag will inform individuals on the level of risk on vacy for their websites and smart phone applications. It w d a global and publicly available knowledge database on lications, websites and smart cities deployments. It will rm the users when his/her privacy is at risk or being eatened by third parties access.
ivities **can include the investigation of measur safeguard privacy in the context of mass data dling,** for example where services exploiting big a, cloud services, data sharing by interconnected ices in the internet of things, and data handling in highly sensitive context of criminal investigations	vacy Flag is structurally scalable by design and precisely nds to assess huge number of websites and smart phon lications that may be connected to cloud-based services ombining: tributed agents to monitor and assess the privacy risk le very high number of smart phones and web browsers; wd sourcing technologies and privacy risk assessment thodology; tributed privacy enablers; roved privacy-preserving routing protocols to protect inst traffic analysis while using mass data handling vices.
ere relevant, actions can be proposed to apply **vacy-by-design frameworks** for a range of differ lications to promote the usage of privacy enhanc nnology.	vacy Flag will foster the adoption of the privacy-by-desig roach by: rning users on any privacy risk; signing an application which is itself privacy by design pect complete anonymity of users; shing application and website developer to become priva ndly; providing support services for companies to identify t vacy risk and help them turning their solution into priv ndly ones. giving guidance on regulatory issues via webinars ferences addressed to Internet and app develop nufacturers of Operating Systems and app-stores.

III - Overall concept underpinning the project

Personal data protection is becoming a challenge both in terms of privacy and economic exploitation. The European Union has taken the lead in better protecting its citizens against unilateral collection and exploitation of personal data. However, this effort is facing several challenges. Considering the extent of the Internet and smart phone applications, and the fact that the vast majority of those applications are developed from outside the EU, it is rather difficult to effectively impose and extend a privacy mechanism from a top down approach or through a simple technological perspective. Data can be retrieved from a smart phone or a computer in a way which remains invisible to the data owner. Moreover, personal data protection norms and privacy concepts may be perceived as too complex and subtle by many citizens.

Privacy Flag intends to combine crowd-sourcing technologies together with privacy monitoring agents, innovative privacy risk assessment methodology and legal expertise to develop a collective privacy protection framework enabling citizens to better control and protect their personal data. The project will research the potential of crowdsourcing and legal expertise to empower the users to set the desired level of privacy, based on a simple to understand visualisation of the privacy level. The project will develop a crowd-sourcing based process and a set of tools and solution enabling the users to collectively assess and control the level of risk for their privacy in the context of web applications, smart phones applications and Internet of Things deployments. It will provide a new paradigm of privacy risk assessment combining:

- Crowd sourcing model of risk identification and evaluation
- Privacy Risk Area Assessment Tool technology
- Distributed agents to monitor, assess and inform on the privacy risk level of any application
- Full "anonymization" and privacy technology for server connection
- Legal expertise in privacy and personal data protection
- Personal data valuation mechanism
- A voluntary legal binding mechanism for companies located outside of Europe

It will develop a clear methodology and a suite of assessment tools to evaluate the level of risk for privacy and personal data exploitation by third parties for different potential end-users perspectives, including:

- Citizens, which constitute the main target group;
- Companies and SMEs;
- Smart cities and public administrations considering deploying Internet of Things;
- Researchers and research projects to assess their risk level to breach privacy;
- ICT Lawyers and policy makers.

A Universal Privacy Risk Area Assessment Tool (PRAAT) will be designed in order to precisely match the European and international norms and standards related to personal data protection and privacy, while providing a simple and user friendly interface. It will be designed to encompass three targeted domains: websites, smartphones applications, IoT deployments. It will assess the level of risk from different angles. The **UPRAAM methodology will translate complex legal obligations into a user friendly evaluation tool**. By exploiting the UPRAAM methodology and the potential of crowd sourcing, the platform will enable a highly scalable privacy risk identification and assessment, which would not be possible with a regular top down assessment approach. Moreover, by mutualizing the skills and capacities of the crowd, it will reverse and rebalance the asymmetric relationship between individual users in front of large and powerful companies.

The project will benefit from experts in privacy law, mobile applications and Internet of Things, including the International Association of IT lawyers, the Istituto Italiano per la Privacy, as well as experts in end-user participation.

Identified sources of privacy risk may be contacted and invited:

- To benefit from a voluntary in depth risk analysis with a report and recommendations for optimizing their practices in terms of privacy protection (as a paying service with experts, whose parts of the fees will be allocated to support financially the platform maintenance);

- To voluntarily and legally abide to a common set of rules aligned with the European personal data protections norms, in order to extend those norms beyond the European territory.

The platform will provide several user-friendly and freely available tools to the citizens to be accessed:

- As an add-on in their Internet browsers;
- As an Android application on their smart phone;
- As a public website.

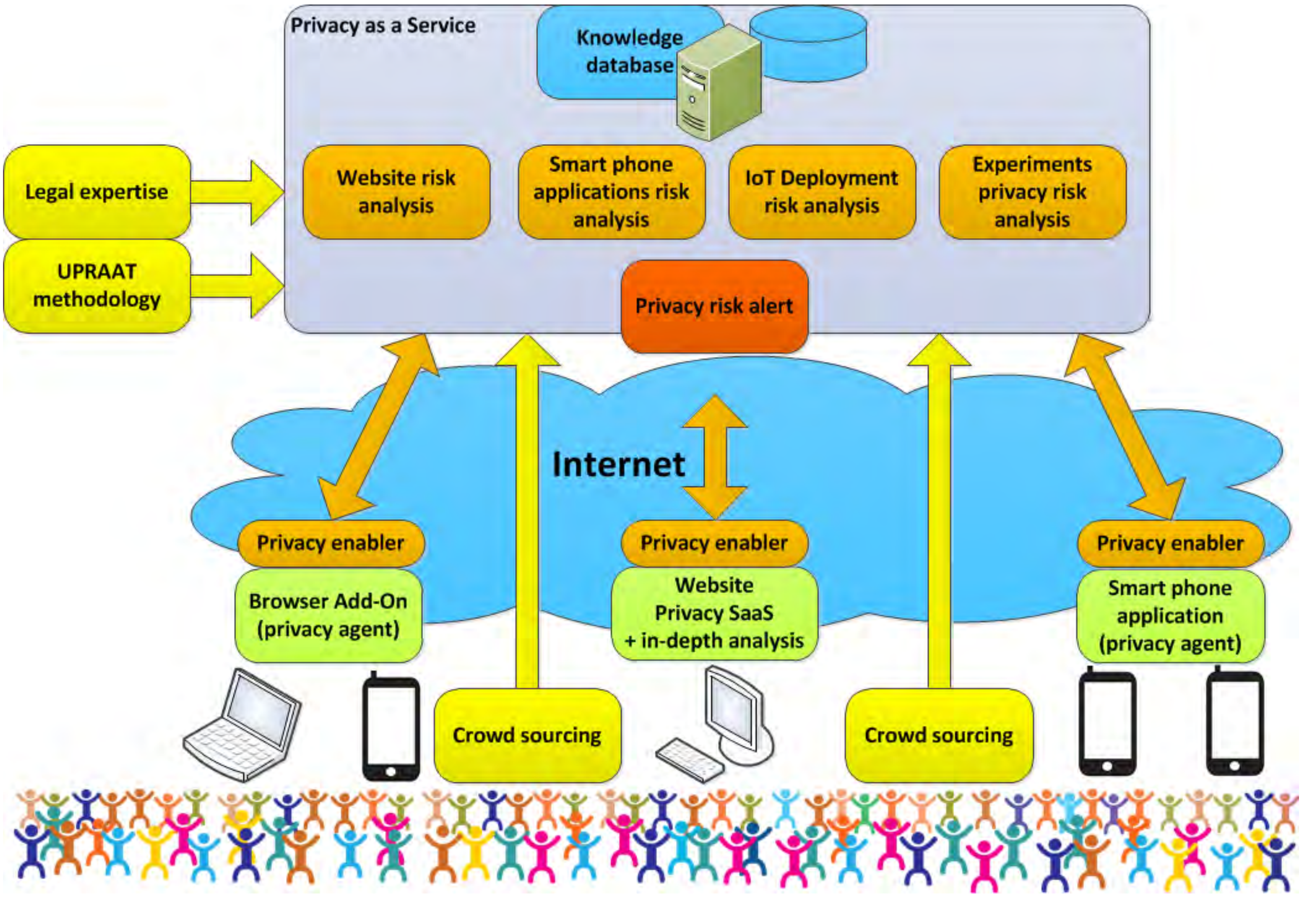

Privacy as a Service
Knowledge database
Legal expertise
UPRAAT methodology
Website risk analysis
Smart phone applications risk analysis
IoT Deployment risk analysis
Experiments privacy risk analysis
Privacy risk alert
Internet
Privacy enabler
Browser Add-On (privacy agent)
Privacy enabler
Website Privacy SaaS + in-depth analysis
Privacy enabler
Smart phone application (privacy agent)
Crowd sourcing
Crowd sourcing

Figure 1: Privacy Flag architecture

The proposed set of tools will include:

- **Distributed agents** locally monitoring and identifying privacy risks.
- **An alert mechanism enabling the crowd:**
  - **to identify** any website, smartphone application or IoT deployment considered at risk;
  - **to be informed on the privacy risk level** of any website, smartphone application or IoT deployment.
- **User friendly privacy risk assessment tools based on the UPRAAM model** for websites, smart phone application and IoT deployments in smart cities;
- **Crowd-sourcing platform** to:
  - Distribute privacy risks assessment with the UPRAAM methodology;
  - Distribute privacy risk identification with the distributed agents;
  - Distribute in-depth risk assessment processes across a community of experts.
- **A Data valuation tool.**
- **A knowledge database** with audited web sites and smart phone applications, with an external assessment of their level of privacy risk; this database will be enriched by the crowd applying the on-line risk area assessment tools.

- **A voluntary legally binding mechanism for companies and public administrations located outside of Europe** enabling them to align with and abide to European standards in terms of personal data protection.
- **On-line resources** to improve privacy, including legal search engine on privacy norms, templates of legal clauses for privacy friendly applications and user agreement, etc.
- **Vulgarization documents** on privacy and data ownership

The platform will also propose: **in depth analysis service, with recommendations and a labelling and certification process**, certifying the compliance with personal data protection and ownership rights. This service will be provided against payment in order to self-finance the maintenance and development of the platform.

In order to support the long term maintenance and exploitation of the platform, a dedicated company aiming at protecting privacy and personal data protection will be set up in Luxembourg, with a branch in Geneva to liaise with ISO, ITU and IEC.

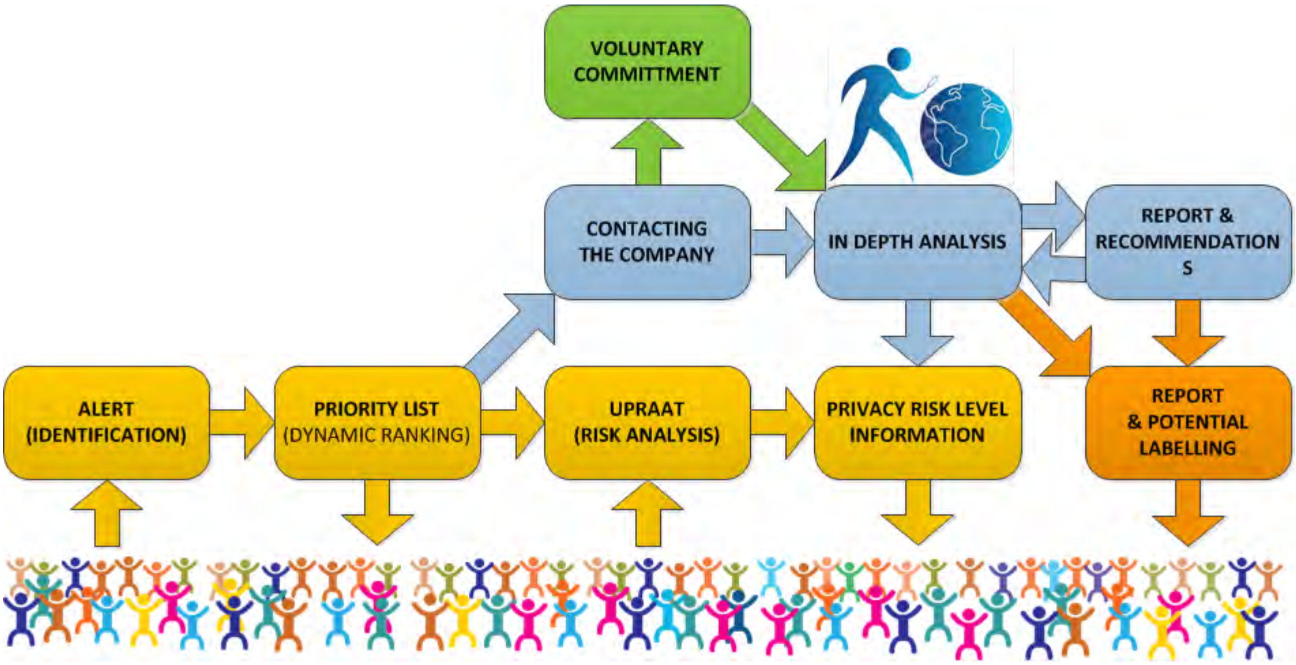

VOLUNTARY COMMITTMENT
CONTACTING THE COMPANY
IN DEPTH ANALYSIS
REPORT & RECOMMENDATION S
ALERT (IDENTIFICATION)
PRIORITY LIST (DYNAMIC RANKING)
UPRAAT (RISK ANALYSIS)
PRIVACY RISK LEVEL INFORMATION
REPORT & POTENTIAL LABELLING

Figure 2: Privacy Flag process

__Main components:__

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.

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 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.

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.

Detailed concepts and proposed innovations

Triple privacy protection focus

Privacy Flag will target three areas of risks threatening privacy and personal data protection:

- Smartphone applications;
- Internet Websites;
- Internet of Things deployments in smart cities.

Combining complementary expertise

Increasing awareness and impacting personal data protection globally require multi-faceted approach, combining legal, societal and technical expertise. In order to address this multidisciplinary topic efficiently, the consortium combines expertise in:

- Privacy and personal data protection (IAIT, IIP, MI)
- Privacy evaluation process (MI)
- Crowd sourcing (MI, CTI, DNET)
- Personal data valuation (Velti, HWC)
- End-user interaction, co-design and empowerment / living labs (LTU)
- Network security (UL, OTE, MI, CTI)
- Anonymization Techniques (UL)
- Smartphone technologies (OTE, Velti, DNET)
- Web technologies (Velti, DNET)
- IoT technologies (MI, DNET, Velti)
- International law and Human Rights (MI, IAITL)
- Standardization (UL, MI, OTE)

Embedding European and international personal data protection norms

Privacy Flag will design and align its architecture in order to be fully compliant with the European societal and legal environment related to privacy. It will take into account international (UN, ITU and OECD related norms) and European standards, including the Charter of Fundamental Rights of the EU (art. 7 and 8), the

Treaty of Lisbon (art. 16, 39, 88, 169), the Directives 95/46/EC, 97/66/EC, 2002/58/EC, 2002/21/EC, 2009/140/EC, 2009/136/EC and Regulations (EC) N°45/2001. Privacy Flag will benefit from:

- IIP, which has a long expertise in personal data protection law, both at European and Italian level, as well as in promoting a constructive dialogue between different stakeholders (industry, regulators, academics, lawyers) with the aim of finding viable practical solutions for the advancement of a culture of respect for individuals' privacy and the adoption of privacy enhancing technologies and privacy–by-design/default approach.
- The International Association of IT Lawyers (IAITL) and its global network of lawyers, legal experts, professors, academic experts, researchers, and policy makers studying the implications and analysis of the regulatory, legal, and compliance issues surrounding Information technology, intellectual Property and telecommunication. IAITL provides our customers, friends and clients the benefits of speedy access to specialist lawyers and a network of dedicated, trustworthy and knowledgeable lawyers with extensive experience in research, long stellar publications, practical experience and legal services. IAITL provides action-oriented guidance by our internationally known legal experts to resolve the problems that users' face, including industry trends which are significant to practice coverage and analysis of important court cases and legal development. IAITL is passionate with our commitment to maximising the immediate and ongoing commercial value of our strategic business partners. Value creation-privacy information security and human respect- are the fundamental principles of our business.
- MI, which has a long expertise in international law and has published several scientific articles on personal data protection, and includes legal experts in its research team. MI has Special consultative status to the UN and is actively participating in the UN Human Rights Council since many years. It is also managing a reference legal search engine on international law: www.whatconvention.org

Privacy Flag will target "privacy by design" approach considering its architecture from a holistic perspective. It will among other limit and exclude personal data, but will also ensure that collected data cannot be reused and combined to rebuild personal data. It will synergize its effort with similar projects having to address the same concern, such as IoT Lab which is coordinated by MI.

Exploiting the potential of crowd sourcing

Privacy Flag will use a crowd sourcing model enabling the users (the crowd) to collectively monitor and safeguard their personal data. By involving all sorts of players with different expertise, the platform will provide a sort of collective intelligence to support privacy protection. Crowd sourcing has a multiple effect:

- Enabling scalability by distributing the evaluation effort across many users (more details below);
- Adapting the effort according to the crowd concerns and priorities;
- Benefiting from the wisdom of the crowd with a large diversity of expertise;
- Raising awareness among the citizens and end-users;
- Building a community of privacy defenders able to influence the public perception on privacy compliance of a given application or website, with a potential impact on the effective use of such solutions. This will constitute a de facto incentive for companies to adapt their product into privacy friendly ones.

Enabling a highly scalable solution

Privacy Flag will design a systemic and scalable by design framework with:

- Work flow scalability through crowd-sourcing, by enabling a distribution of the privacy risk assessment and related workload across a large number of third parties.
- Robustness of a system towards a large number of connection requests and data handling. It will be handled by equipping the platform infrastructure with fault tolerance, high availability and automatic fail-over mechanisms to provide uninterruptible service time to the platform users and sustain large number of connection requests, even during peak system usage periods. Open source technologies for cloud will be used in order to make the server and data storage scalable too.
- Social scalability with the ability to encourage and attract a very large numbers of users. It will provide a fast, user friendly and transparent registration process implemented by a transparent and lightweight

module. Privacy Flag will provide its own download section to download and install its application from its website. However, in order to extend its outreach, Privacy Flag will use mainstream app store, such as Google Play, while mitigating the risks that such platform be itself used to collect personal data on the Privacy Flag users.

Universalizing the Privacy Risk Area Assessment Tools methodology

Privacy Flag will further research, adapt and exploit the Privacy Risk Area Assessment Tool methodology developed by the EAR-IT research project for audio monitoring[i]. It was designed to assess the risk of breaching personal data protection and other privacy-related norms when deploying audio monitoring solution. It relies on an iterative assessment tool which enables to assess, identify and mitigate such risks. The solution will be fully redesigned to encompass all sorts of privacy-related risks, overpassing the audio monitoring context. It will end up in providing a Universal Privacy Risk Area Assessment Tool (UPRAAM) to be used by the crowd and by experts in order to assess the risks related to websites, smart phone applications and Internet of Things deployments in smart cities.

Integrated approach to protect privacy

The Privacy Flag will impact privacy and personal data protection through several channels, by:

- Providing a user friendly privacy risk monitoring and protection platform for citizens;
- Making legal norms and obligations on privacy understandable by a large public;
- Promoting the platform through the medias and other relevant channels, such as consumers associations;
- Raising awareness and changing the behaviour of participating citizens, enabling them to understand how they can better protect their privacy;
- Providing a highly scalable platform that can be easily extended to other risk areas;
- Empowering users to take the leadership on their privacy by easy-to-use ICT tools;
- Enabling for better understanding and knowledge among companies and organizations on privacy respect.

User empowerment

Privacy Flag aims to endow users with tools that help them to manage their online privacy from different perspectives. On the one hand users can *assess privacy risks in different digital solutions* and by this take an active role as digital citizens, on the other hand *become informed* on privacy risks of different websites and mobile applications to take their own decision on risks in use and finally to take *the leadership in their digital human right*. These are the main perspectives of user empowerment principles to foster users as actors of their digital society and giving the users the power of their privacy rights.

Active involvement of citizens in improving their personal data protection

In this project we will apply existing SoA in user-involvement involving the users from early needfinding, concept-design and co-creation to experimentation (field-trials) and evaluation. We will apply an iterative Experiential Design process to support the design for user experience while sharing knowledge and crystallizing the collective intelligence of the users. Hence, new concepts, artifacts and solutions emerge from the resulting increase of knowledge acquired through accumulated experiences. It is not only targeted to evaluate the user experience but also to co-create and explore value propositions that are intended to enhance the user experience and Privacy Flag usefulness and scalability.

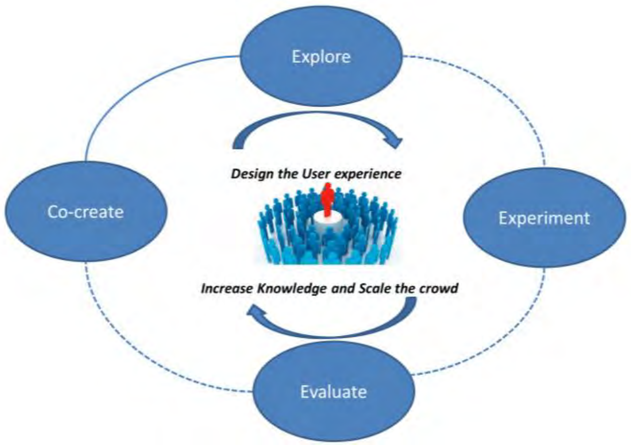
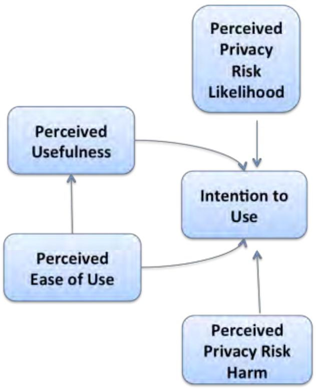

Explore
Design the User experience
Co-create
Experiment
Increase Knowledge and Scale the crowd
Evaluate

Figure 3: Technology Acceptance Model and Privacy

(Cazier et al., 2007)

Building outreach and end-user acceptance


Perceived Privacy Risk Likelihood
Perceived Usefulness
Intention to Use
Perceived Ease of Use
Perceived Privacy Risk Harm

There is a huge mass of literature covering the area of adoption and acceptance of innovations both in organisations and among individuals[i, ii, iii, iv, v, vi, vii]. The acceptance of innovation is in many cases only referring to the process of buying an innovation, but acceptance also includes using the innovation[viii]. Research about factors that can lead to adoption and acceptance is wide and multidisciplinary[ix, x] . For example, within marketing the focus is often on how consumers perceive the innovation[xi], while in New Product Development (NPD) the focus is on which features of an innovation are most critical to achieve market success[xii], and in sociological studies the focus is on how technology adoption is affected by characteristics in the society[xiii]. In general, technology adoption is a multidimensional process where individual's behaviour is influenced by a variety of conditions. These conditions can be learning, social and technological conditions. Firstly, learning conditions are individual characteristics of a single user. These conditions can be expected to have influence on the attainment of new competencies needed to use the new technology. Secondly, social conditions explain the cultural and relational specifies shared within the communities to which the user belongs. Thirdly, technological conditions can be perceived ease of use, usefulness, trust that facilitates the explanation of technical features of the exchanging technology.

To increase the level of acceptance and adoption of the technology being developed in this project, it is important to understand the values and motivators that drives the end-users to use technology and to contribute with their insights and experiences of using different websites and applications as a crowd. In previous research[xiv], motivating factors that stimulate crowds to contribute in innovation activities are cause, achievements, social, and, efficacy and learning.

To date, crowd engagement processes have proven successful in different phases of an innovation and development process, such as idea generation, co-design, and tests and evaluation of innovations in the different contexts and for different purposes. Most research in this area has focused on engaging crowds to do some predefined work, for instance in Amazon Mechanical Turk, to compete in idea competitions or design contests as well as collaboratively create something as for instance Wikipedia. In this project, the crowd will be engaged in activities such as identify and alerting on risks, assessing risks and make suggestions for their prevention.

In order to be able to attract and engage a large crowd of end-users we will develop specific strategies for this during the project since there is an extreme competition of users on the web. Contributing to these types of activities reflects a conscious strategic decision by end-users to become involved in crowd sourcing activities. In order to understand how to engage users in these co-creative activities it is important to understand the mechanisms behind their behaviour and how incentives can be used to stimulate end-users to participate and contribute.

Privacy monitoring agents

Privacy Flag will develop a privacy monitoring agent to be embedded in the smart phone application and the web browser add-on. This agent will monitor the local activity in order to identify suspicious activities related to personal data protection. It will use different parameters, including configuration settings monitoring, data traffic, network activity, etc. The Privacy monitoring agent will enable to inform the user about any identified threat as well as to feed the central knowledge database on suspicious applications and websites to be analyzed.

Privacy and security enablers

Walking the talk is essential for the credibility of the project. In order to optimize the privacy protection of the platform users, we will increase privacy protection with a set of privacy enablers. We will design our approach by leveraging on privacy preserving authentication technologies, such as Privacy-ABCs[xv], as well as TCP/IP security protection mechanisms, which include TLS/SSL and IPSEC. All platform services will employ HTTPS connections while the platform will be safeguarded by intrusion detection and handling modules. More specifically, we plan to provide the users with a dedicated set of tools to increase their level of anonymity when using smart phone application or visiting websites. The architecture will rely on a fully anonymized user registration.

Anonymization for privacy

Traditional communications security protects the confidentiality and integrity of the content of communications. The techniques to fulfill this goal have now reached a certain level of maturity (even though using information from patterns in the communication, it is sometimes possible to deduce information about contents of the communication, e.g., applying the so-called fingerprinting techniques). However, secure communications systems still leak information about the routing of messages in the network (who is talking to whom, time and volume of data transmitted, chat initiation and replies, on-line presence), that may be used by adversaries to gain intelligence. We will develop and evaluate efficient methods for network layer anonymization that are able to meet current challenges in terms of both, quality of protection and quality of service.

IPv6 Privacy Extension

The privacy of auto configured IPv6 addresses using the interface identifier was an issue discussed in the IETF in the early days of IPv6. If an IPv6 address is built using the MAC identifier, the Internet access could be traced even across networks, because this identifier is unique to your interface. It is important to understand that an IPv6 node can have an address based on the interface identifier, but this is not a requirement. As an alternative, the IPv6 device can have an address like the ones currently used with IPv4, either static and manually configured or dynamically assigned by a DHCP server. RFC 4941, "Privacy Extensions for Stateless Address Auto configuration in IPv6," introduces another type of address available only in IPv6 that contains a random number in place of the hardware address. This interface ID can also change over time. It is sometimes also called a *temporary address*. It is generated in addition to the EUI-64 interface ID. We will carefully analyze privacy capabilities and challenges of using IPv6 and come up with thorough recommendations and solutions.

DNSSec Security for privacy

The original DNS was designed to be scalable but without any security in mind. The practical deployment of the system opened many vectors for attacking the system. As an answer, DNSSec was designed to protect applications from using forged or manipulated DNS data. The idea is to use certificate chains similar to those with SSL certificates. Although the goal of DNSSec is to increase security, it introduces a new problem that many believe is a privacy vulnerability: the zone enumeration (also known as "zone walking") issue. DNSSec forces the exposure of information that by normal DNS best practice is kept private. All the so far existing solutions to address this issue do not eliminate this issue, but rather makes it harder for the attacker. Because of this issue, it is unclear whether DNSSec is legal to deploy in many countries. DENIC has stated that DNSSEC's zone enumeration issue violates Germany's Federal Data Protection Act. Other European countries have similar privacy laws forbidding the public release of certain kinds of information. We will analyse the state of affairs with DNSSec with respect to privacy and research possibilities to deploy systems that are able to meet arising challenges.

Personal data valuation tool

In 2012 the Boston Consulting Group stated in their report The Value of Our Digital Identity[xvi] the current and potential economic value of the digital identity to €1 trillion in Europe by 2020. For European businesses and governments it was foreseen to deliver an annual benefit of €330 billion by 2020. For individuals, the value was estimated be more than twice as large: €670 billion. So personal data is valuable and the value is dependent on three things: Accuracy, Validation, and Context. The Privacy Flag Personal data valuation tools are suggested to be designed in close interaction with the end-users. The first step will be to start by identifying user-needs and to explore available privacy feedback and awareness tools and then to integrate and adopt them to fit different individual preferences. The tools must enable users to control their personal data. The proposed tools should also raise the user's awareness concerning both her privacy and of the economic value of her information and to assist her in managing her personal data. From the Boston report it was found that only 10% of respondents have ever taken six or more out of eight common privacy-protecting measures, such as changing their privacy settings in a social network or opting out of certain data uses. Therefor the personal data valuation tools must support to activate users to become privacy aware but also to make users to take active decisions on which personal data to share, with whom and why and under which circumstances.

Smartphone application

During the last years, the growth of smart devices and mobile apps has exploded. The majority of mobile apps is stored on and delivered from mobile app stores that are operated by Apple (iTunes App Store), Google (Google Play), Microsoft (Windows Phone Store) and BlackBerry. The number of available apps on Google Play is 1,254,516[xvii], while the iTunes App Store has 1.2 Million Apps, and has seen 75 Billion Downloads to date[xviii]. All these applications monitor and exploit different types of user information that is directly or indirectly provided (user inputs, GPS location etc) for advertisement or service provision purposes. The Privacy Flag project will provide the solutions to identify privacy leaks of smartphone applications and assess the level of end user privacy risks. The settings of the user device as well as the data flows to and from the installed applications (e.g., monitoring applications' log files) will be exploited for that purpose. Special attention will be paid to social-enabled applications. Furthermore, in the near future smartphone applications will be capable of sending and receiving data automatically via the internet from IoT devices in the context of a smart city environment. The potential of IoT is a key challenge for the Privacy Flag, since important privacy issues arise, especially in the case that applications interact e.g., with wearable devices.

Web browser add-on

This is a key technical enabler for the Privacy Flag ecosystem. Web browser is one of the applications that have revolutionized the Internet and World Wide Web, enabling the presentation, the traversal and the exchange of all types of information resources (financial, health, entertainment etc). In many cases, all this information is tracked and used by third parties without receiving the end user consensus. Hence, the existence of a Web Browser add-on for users protection is necessary and its role is twofold; on the one hand it operates as end-users' real-time behavioural and personal browser data collector, while on the other hand it helps users to identify the trackers of their web browser and then define fine-grained "do not track rules". Users' personal and behavioural data generated via the web browsers, either explicitly or implicitly, are given as input to the privacy risk area assessment tools for users' privacy protection. The latter provides warnings for the level of privacy risk. The Privacy Flag Web Browser add-on will also track users' trackers, (i.e., third party online tracking and analytics services) that monitor and collect end-users digital trail on their web browser(s). Mobile web browsers will be also considered in the Privacy Flag project due to mobile devices' special characteristics.

Global Privacy risk knowledge database

There are various sources of information that are directly or indirectly created by the end users and may be used by trackers or third party applications, increasing privacy risks for the users. The collected and filtered data from various crowd sources (web browsers, smartphone applications, IoTs) are accumulated in the Privacy Flag knowledge database in order to facilitate their correlation as well their processing at different timescales. After the application of the Privacy Risk Area Assessment methods, the knowledge database stores the levels of risk for privacy and personal data exploitation for specific users, types of crowd sources or even for specific crowd source objects (i.e., specific web browser trackers, or specific applications) that could be uniquely identified (e.g., smartphone application name).

Voluntary and legally binding commitment

Organizations and companies located within the EU territory are bound be the European norms and standards, which is not the case for entities based outside of Europe. There is a risk of gap in terms of privacy protection according to the geographic location of the entity. For organizations located outside EU, a voluntary legal binding mechanism will be drafted and made available under the project. Designed for organizations located outside of Europe, formal adoption of this 'compliance commitment tool' will enable them to signify their legal abidance to a common set of rules aligned with the European personal data protections norms, in order to extend those norms beyond the European territory.

In depth privacy risk analysis, labelling and certification

Privacy Flag will provide an in-depth privacy risk analysis to interested companies. It will be based on an extended and more detailed version of the UPRAAM enabling experts to provide a systematic evaluation of the application or website privacy risk. It will enable to advise companies in improving the privacy friendliness of their solutions. Moreover, for companies whose products are fully compliant with the UPRAAM requirements a labelling and certification process will be proposed. The certification process will be aligned with ISO models and practices and a potential cooperation with ISO will be explored.

Didactic personal and fully anonymised report on privacy risk level

The application will enable the user to locally collect data on the risks identified by the application during a period of time. This will enable the end-user to assess its exposure to privacy breach and data exploitation by third parties, and to assess how this risk has evolved over time. This tool will also suggest simple and practical measures to reduce this exposition, as well as an optional list of application at risk. This will be a key enabler for user awareness and education.

[i] EAR-IT FP7 Research project : www.ear-it.eu

[ii] Devaraj, S., Easley, R.F., and Crant, J.M., (2008). "Research Note--How Does Personality Matter? Relating the Five-Factor Model to Technology Acceptance and Use". INFORMATION SYSTEMS RESEARCH, 19(1): p. 93-105.

[iii] Lee, D. and Mendelson, H., (2007). "Adoption of Information Technology Under Network Effects". INFORMATION SYSTEMS RESEARCH, 18(4): p. 395-413

[iv] Parthasarathy, M. and Bhattacherjee, A., (1998). "Understanding Post-Adoption Behavior in the Context of Online Services". INFORMATION SYSTEMS RESEARCH, 9(4): p. 362-379

[v] Se-Joon, H. and Kar Yan, T., Understanding the Adoption of Multipurpose Information Appliances: The Case of Mobile Data Services, in Information Systems Research. 2006, INFORMS: Institute for Operations Research. p. 162-179.

[vi] Venkatesh, V. and Ramesh, V., (2006). "Web and Wireless Site Usability: Understanding Differences and Modelling Use". MIS Quarterly, 30(1): p. 181-205.

[vii] Wixom, B.H. and Todd, P.A., (2005). "A Theoretical Integration of User Satisfaction and Technology Acceptance". INFORMATION SYSTEMS RESEARCH, 16(1): p. 85-102.

[viii] Langley, D., . J and Pals, N., (2005). "Adoption of Behaviour: Predicting Success for Major Innovations". European Journal of Innovation Management, 8(1): p. 55-78

[ix] Beaudry, A. and Pinsonneault, A., UNDERSTANDING USER RESPONSES TO INFORMATION TECHNOLOGY: A COPING MODEL OF USER ADAPTATION, in MIS Quarterly. 2005, MIS Quarterly & The Society for Information Management. p. 493-524.

[x] Jasperson, J., Carter, P.E., and Zmud, R.W., A COMPREHENSIVE CONCEPTUALIZATION OF POST-ADOPTIVE BEHAVIORS ASSOCIATED WITH INFORMATION TECHNOLOGY ENABLED WORK SYSTEMS, in MIS Quarterly. 2005, MIS Quarterly & The Society for Information Management. p. 525-557.

[xi] Wang, W. and Benbasat, I., INTERACTIVE DECISION AIDS FOR CONSUMER DECISION MAKING IN E-COMMERCE: THE INFLUENCE OF PERCEIVED STRATEGY RESTRICTIVENESS, in MIS Quarterly. 2009, MIS Quarterly & The Society for Information Management. p. 293-320.

[xii] MacVaugh, J. and Schiavone, F., (2010). "Limits to the diffusion of innovation: A literature review and integrative model". European Journal of Innovation Management, 13(2): p. 197-221

[xiii] Selwyn, N., (2003). "Apart from Technology: Understanding People's Non-Use of Information and Communication Technologies in Everyday Life". Technology in Society, 25(1): p. 99-116.

[xiv] Carpenter, H., (2011), "Motivating the Crowd to Participate in Your Innovation Initiative", in A guide to open innovaiton and crowdsourcing; Advice from leading experts, Sloan, P., Editor. KoganPage: London.

[xv] The ABC4Trust project. https://abc4trust.eu/

[xvi] Boston Group, The Value of Our Digital Identity (Nov 2012)

[xvii] "Number of Android applications", http://www.appbrain.com/stats/number-of-android-apps

[xviii] "iTunes App Store Now Has 1.2 Million Apps, Has Seen 75 Billion Downloads To Date", http://techcrunch.com/2014/06/02/itunes-app-store-now-has-1-2-million-apps-has-seen-75-billion-downloads-to-date/