Privacy Flag – Collective Privacy Protection Scheme Based on Structured Distributed Risk Assessment

Introduction to the Privacy Flag European Research project

Sébastien Ziegler
Mandat International
Geneva, Switzerland
sziegler@mandint.org

Latif Ladid
University of Luxembourg
Luxembourg, Luxembourg
latif@ladid.lu

Ioannis Chochliouros
Hellenic Telecommunications Organization SA OTE
Athens, Greece
ichochliouros@oteresearch.gr

***Abstract*— This article presents the Privacy Flag European research project model for privacy and personal data protection. The project is researching and developing an innovative model of privacy protection based on crowdsourcing, and combining human and technical distributed control and monitoring of privacy-related risks. The project focuses more specifically on Internet of Things deployments, smart phone applications and websites. It further develops the Privacy Risk Area Assessment Tool (PRAAT) developed by Mandat International in the context of the EAR-IT research project with an international research team combining expertise in law, personal data protection, security and ICT in general.**

Keywords*— *Privacy, Personal data protection, Internet of Things, crowdsourcing, smart phone applications, websites, Privacy Risk Area Assessment Tool.

I. INTRODUCTION

Privacy Flag (www.privacyflag.eu) [1] is a 3 years Horizon 2020 European Innovation Action. It 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 intends to enable citizens to collectively monitor and control their privacy with a user friendly solution made available in three distinct options: as a smartphone application, a web browser add-on, and a public website,- all connected to a common knowledge database. It provides 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 incentives for companies to improve their privacy compliance.

II. LEGAL AND POLITICAL ENVIRONMENT

As highlighted in [2], Privacy and personal data protection enjoy legal protection from several core international treaties and conventions, including the Universal Declaration of Human Rights of 1948 (UDHR) [3] and the International Covenant on Civil and Political Rights (CCPR) [4]. Several treaties related to specific groups of persons and specific domains contain similar binding commitments in their core text, such as the Convention of the rights of the Child [5], the International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families [6], and the Convention on the Rights of persons with disabilities [7]. The International Telecommunication Convention provides a complementary set of obligations with a focus on communications. All these basics texts are quite consistent and set the basis for a fundamental principle: The obligation for members States to protect individuals against arbitrary or unlawful interferences or attacks with their privacy [8] and the obligation to protect secrecy in international correspondence and communications [9]. These obligations are formally and materially binding the ratifying parties.

At the regional level, the European Union has developed a specific normative framework to further protect personal data protection of its citizens. The right to personal data protection is anchored in Article 8 of the Charter, Article 16 of the Treaty on the Functioning of the European Union (TFEU), and Article 8 of the European Convention on Human Rights **(**ECHR). It is completed by a set of secondary norms, including regulations and directives, such as the European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. This Directive *"sets strict limits on the collection and use of personal data and demands that each Member State set up an independent national body responsible for the protection of these data."* [10] It is completed by a set of

specific directives mainly on data access and electronic communications in order to ensure that citizens and users can trust their authorities as well as "*the services and technologies they use for communicating electronically"* [11]. Other norms have an impact on privacy rights, including Council Regulations, Communications, Recommendations (such as the Recommendation 2006/952/EC for the protection of minors and human dignity in audio-visual and information services), and opinions given by the Working Party of the data protection framework.

Furthermore, the European Union is currently working on a new set of obligations, the Data Protection Regulation, which will extend the norms in favor of citizen personal data protection. It will extend the scope and level of penalties for companies breaching these obligations [12].

Despite the legal framework evolving towards stricter and deeper obligations, the effectiveness of such norms remains an issue.

III. PRIVACY FLAG OBJECTIVES

Privacy Flag has designed a new paradigm able to address this scalability issue. Its 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: Internet of Things deployments in smart cities, websites, and smartphones applications. Privacy Flag is pursuing several complementary objectives and will:

1. Develop a highly scalable privacy monitoring and protection solution based on:
   - Crowdsourcing 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;
   - 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.
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.
3. Develop a set of complementary tools and services, including:
   - In-depth privacy risk analytical tool and services;
   - Voluntary legally binding mechanism for companies located outside of Europe to abide to European standards in terms of personal data protection;
   - Services for companies interested in being privacy friendly;
   - Labelling and certification process and service.

IV. SCALABLE CROWD-DRIVEN MODEL

With a growing omnipresence of ICT technologies and a pervasive Internet of Things, identifying and assessing the sources of risk for one's privacy is a Sisyphean task: over 50 Billion IoT devices to be deployed by 2020, about a Billion websites [13] and a growing number of smartphone applications estimated to over 3'730'000 [14]. In this context, a centralized approach to identify and assess the level of risk is not realistic even with massive financial resources. This has pushed projects and platforms such as MyWot [15] to rely on on crowdsourcing models. However, the inputs provided by the crowd are mainly based on subjective appreciations.

Privacy Flag is built on an innovative and structured methodology for privacy risk assessment, which can be applied by non-specialists, while providing a sound and factual-based assessment of the level of risk and compliance with personal data protection. Moreover, it combines a user-centric assessment together with privacy monitoring agents. In brief, Privacy Fag intends to combine the power of the crowd with innovative methodological approach for risk assessment and technical enablers.

V. TECHNICAL APPROACH

Privacy Flag is combining several enablers into a comprehensive platform:

A. Universal Privacy Risk Area Assessment Tools

Privacy Flag is further extending the Privacy Risk Area Assessment Tool (PRAAT) [16] [17] designed by Mandat International [18] in a previous European research project, EAR-IT, which was researching audio monitoring in smart cities and smart buildings [19].

The personal data protection obligations are rather complex. In order to tackle this complexity, the PRAAT has identified and defined a few concepts and a practical tool enabling an easier evaluation of the risks related to audio monitoring deployment. It defines the concept of "Privacy Risk Area" as an area in which the risk to breach someone's privacy rights is high. By opposition, a "Privacy Safe Area" is an area in which the risk to breach someone's privacy rights is very low. A grey zone area is implicitly emerging between those two previous notions, where the level or risk to breach someone's privacy rights is not clearly identified. (See figure 1)

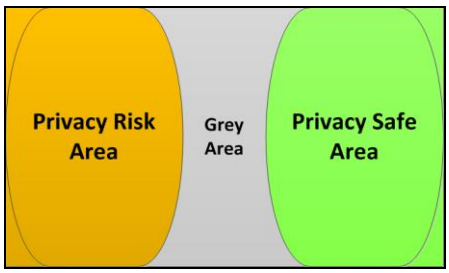

Figure 1. Privacy Risk Area (PRA) and Privacy Safe Area (PSA)

Based on those concepts, the Privacy Risk Area Assessment Tool (PRAAT) provides a user friendly tool which enables any researcher or public administration without legal background to estimate if a planned audio monitoring deployment is rather compliant with privacy obligations (in a Privacy Safe Area) or likely to breach some privacy rights (in a Privacy Risk Area). The proposed tool does not pretend to provide an absolute answer, but a highly accurate estimation of the privacy compliance. The Privacy Risk Area Assessment Tool (PRAAT) is a multi-criteria assessment tool based on a two steps analysis:

1. Preliminary check

   A PRA Preliminary check is proposed, where the user is invited to check a first list of criteria. If the answers provided by the user comply with all the criteria, the assessed solution should be in a rather Privacy Safe Area and the PRAAT considers that the analysis can be stopped there. If one or several of the above criteria is not respected, the assessed solution will most likely trigger obligations related to personal data protection. Hence, a second set of criteria is presented to the user, in order to assess if the experiment remains in a privacy safe area.

2. Complementary check

   If the preliminary check failed, a complementary check list of questions is submitted to the user. If the assessed solution or plan matches all those criteria, it is considered to be in a Privacy Safe Area. If not, it has a high probability to be either in a Privacy Risk Area or in a grey area.

The PRAAT methodology enables the user to focus on the key factors of risk. In case of an unsuccessful result, the PRAAT methodology preconizes an iterative process. The user is invited to examine the key factors having caused a negative result and consider some adaptation to the deployment plan in order to mitigate those risks. Then the PRAAT should be then applied again to the adapted deployment plan. If despite the iterative process (see Figure 2) the result remains negative, a deeper analysis and consultation with the competent authorities is required.

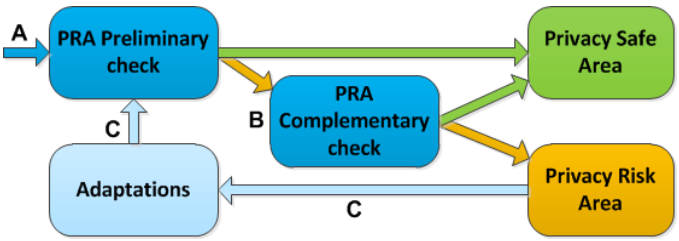

Figure 2. PRAAT iterative process scheme

While the PRAAT was specifically designed to address privacy risks related to audio monitoring, Privacy Flag will further extend this approach by designing a Universal Privacy Risk Area Assessment Tools (UPRAAT), which will be made available to the crowd to assess the level of risk on their privacy with specific websites, smartphones applications and Internet of Things deployments in smart City. Together with its legal experts, it will translate complex norms into a user friendly evaluation tool to be used by the public at large and accessible to non-specialist. It will encompass various application domains, cinluding: Internet of Things deployments in smart cities, websites and smart phone applications. A complementary UPRAAT version will be designed for researchers in order for them to self-assess the privacy risks related to their planed experiment.

The UPRAAT methodology will also serve as a basis to develop an in-depth evaluation tool to be used by experts in the context of labelling and certification on privacy norms compliance. This dimension will be further researched with Archimede Solutions, one of our partners, which has initiated the Euro Privacy certification and support service on privacy and personal data protection compliance [20].

B. A distributed platform for privacy risk monitoring

Leveraging on the UPRAAT methodology, Privacy Flag is developing a 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 designed platform 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.

Privacy Flag is developing three components enabling direct interactions with the crowd through distinct interfaces:

- A Privacy Flag browser add-on to be included in the user's web browser;
- A Privacy Flag Smartphone application;
- A Privacy Flag 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 crowdsourcing platform.

The latter one will provide access to complementary information on privacy protection and resources, and will be accessible through the two former ones.

The three above mentioned tools will enable the crowd to trigger an alert on any suspicious application, website or unusual deployment of IoT devices in a smart city that could constitute a risk to privacy. The list of alert will be dynamically ranked according to the number of alerts received for each individual object to be assessed. It will enable the crowd to rank and prioritize the risk evaluation process according to the users' priority concerns.

C. *Privacy Monitoring Agents*

Privacy Flag will also research and develop Privacy Monitoring Agents (PMA) as software components to be deployed on users' devices for monitoring and detecting suspicious smartphone applications or websites 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.

D. *Putting the citizens at the core*

The role of the crowd is central in the Privacy Flag model:

1. The crowd starts spotting and identifying suspicious smartphone applications, websites and Internet of Things deployment;
2. The crowd then implicitly enables automatic ranking of the objects to be assessed according to the number of clicks/alerts received by the crowd;
3. Member of the crowd then contribute to assess the objects of concern according to a clear methodology, by applying the Universal Privacy Risk Area Assessment Tool methodology;
4. The crowd mutualize and share the collective knowledge generated by the users into a common knowledge data base benefitting to all the users;
5. The crowd finally contributes to disseminate and outreach the platform and tools.

E. *Voluntary and legally binding commitment*

Websites and smartphone applications are global by nature. However, while organizations and companies located within the EU territory are directly bound be the European norms and standards, it is not the case for entities based outside of Europe. Even if the new European norms on personal data protection will impact companies based outside of Europe as soon as they start collecting data from European citizens, there is a risk of gap in terms of privacy protection according to the geographic location of the entity.

Privacy Flag is working on a new approach. It is designing a voluntary legal binding mechanism for organizations located outside EU. 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.

VI. EXPECTED OUTCOMES

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

- A distributed privacy risk monitoring platform based on three user-friendly tools for citizens: a smartphone application, an add-on for Internet browsers and a public website.
- The Universal Privacy Risk Area Assessment Tool (UPRAAT) 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. The UPRAAT methodology will translate complex legal obligations into a user-friendly evaluation tools. It will enable the crowd to use the UPRAAT 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.
- A set of 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.
- A global knowledge database on privacy risks indexing websites, smart phone applications and IoT deployments, fed by the crowd (applying the UPRAAT), by alerts received from the Privacy Flag distributed monitoring agents, and by experts performing in-depth risk evaluations.
- A 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.

Finally, a labelling and certification process will be considered in parallel to cooperation with standardization development organizations.

VII. Expected Impact

By combining the UPRAAT methodology, distributed privacy monitoring agents and crowdsourcing, 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. More generally, Privacy Flag intends to provide a set of tools and services to improve personal data protection and privacy of citizens.

VIII. Consortium

Privacy Flag gathers 12 European partners combining complementary technical, legal, societal, business expertise, including in crowdsourcing, personal data protection, security, data valuation and end-user acceptance. The partners include 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.

Acknowledgment

This article has been written in the context of the Privacy Flag Horizon 2020 European Project, which is supported by the European Commission and the Swiss State Secretariat for Education, Research and Innovation. The opinions expressed and arguments employed do not engage the supporting parties.

References

[1] Privacy Flag is a European Research project of the Horizon 2020 research programme of work, supported by the European Commission, with complementary support from the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract 15.0165. The opinions expressed and arguments employed do not necessarly reflect the official views of the European Commission or of the Swiss Governement.

[2] Ziegler S., Sonko P., Privacy Risk Area Assessment Tool for Audio Monitoring – from legal complexity to practical applications, Journal of International Commercial Law and Technology (JICLT) Vol.9, No.3 (2014)

[3] The Universal Declaration of Human Rights, http://www.ohchr.org/EN/UDHR/Documents

[4] International Covenant on Civil and Political Rights, New York, 16 December 1966 at http://treaties.un.org/pages/CTCTreaties;

[5] Convention on the Rights of the Child, http://www.ohchr.org,

[6] Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, http://www2.ohchr.org/english/bodies

[7] http://www.un.org/disabilities/convention

[8] Article12 and Article 17 of the UDHR and International CCPR respectively

[9] International Telecommunication Convention Concluded at Nairobi, 1982

[10] http://europa.eu/legislation_summaries

[11] http://europa.eu/legislation

[12] The EU data protection reform is currently drafting a new set of norms, the Data Protection Regulation, that will replace and extend the existing ones. More information available on: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

[13] 955’348’530 websites on June 11 2015, according to http://www.internetlivestats.com/total-number-of-websites/ and http://www.internetlivestats.com/

[14] 3’730’000 apps on June 11 2015, according to http://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

[15] MyWot, http://www.mywot.com

[16] Ziegler S., Sonko P., Privacy Risk Area Assessment Tool for Audio Monitoring – from legal complexity to practical applications, Journal of International Commercial Law and Technology (JICLT) Vol.9, No.3 (2014)

[17] Ziegler S., Sonko P., Malo P., Privacy Risk Area Assessment Tool for Audio Monitoring – providing a pragmatic solution, ICT Law, in 2013

[18] Mandat International, http://www.mandint.org

[19] EAR-IT European research project, http://www.ear-it.eu

[20] Euro Privacy certification service pioneered by Archimede Solutions: http://www.europrivacy.org