*Legal Knowledge and Information Systems*
*S. Villata et al. (Eds.)*


*doi:10.3233/FAIA200881*

# CAP-A: A Suite of Tools for Data Privacy Evaluation of Mobile Applications

Ioannis CHRYSAKIS [a,b], Giorgos FLOURIS [a], George IOANNIDIS [c], Maria MAKRIDAKI [d], Theodore PATKOS [a], Yannis ROUSSAKIS [a], Georgios SAMARITAKIS [a], Alexandru STAN [c], Nikoleta TSAMPANAKI [a], Elias TZORTZAKAKIS [a], and Elisjana YMERALLI [a]

[a] *FORTH, Institute of Computer Science, Greece*
[b] *IDLab, Dept. of Electronics and Information Systems, UGent, imec, Belgium*
[c] *IN2 Digital Innovations GmbH, Germany*
[d] *FORTH, PRAXI Network, Greece*

**Abstract.** The utilisation of personal data by mobile apps is often hidden behind vague Privacy Policy documents, which are typically lengthy, difficult to read (containing legal terms and definitions) and frequently changing. This paper discusses a suite of tools developed in the context of the CAP-A project, aiming to harness the collective power of users to improve their privacy awareness and to promote privacy-friendly behaviour by mobile apps. Through crowdsourcing techniques, users can evaluate the privacy friendliness of apps, annotate and understand Privacy Policy documents, and help other users become aware of privacy-related aspects of mobile apps and their implications, whereas developers and policy makers can identify trends and the general stance of the public in privacy-related matters. The tools are available for public use in: `https://cap-a.eu/tools/`.

**Keywords.** data privacy, privacy evaluation, mobile applications, crowdsourcing

## 1. Introduction

We experience a massive increase in personal information utilised by smartphone applications, whose invasive nature for harvesting personal data (despite the recently-imposed GDPR legislation) has been demonstrated in many studies. Apps typically analyze their privacy behavior in Privacy Policy (PrP) documents, which describe, in legal terms, the critical privacy-related aspects of the app, such as the types of personal data being accessed, or the way they are being used. However, PrP documents are typically lengthy, difficult to read (containing legal terms and definitions [1]) and frequently changing[1]; a recent study by the Norwegian Consumer Council showed that just reading these documents for apps on a typical smartphone would take several hours[2].

Considering the scope, length and complexity of PrP documents, it comes as no surprise that the average consumer is not investing sufficient time to study such a doc-

[1] https://www.varonis.com/blog/gdpr-privacy-policy/
[2] http://www.forbrukerradet.no/side/the-consumer-council-and-friends-read-app-terms-for-32-hours/

ument before agreeing to it, thus unintentionally granting permission to apps to access and process a wealth of personal information in an unknown manner.

The CAP-A project[3] aims to *support the average user in the daunting task of understanding the content of a PrP document, and to be aware of the privacy implications of using any given mobile app*. This is done through a set of tools employing crowdsourcing techniques to support users in expressing their privacy concerns and expectations, annotating PrP documents, and better understanding privacy-related information regarding the used apps. Developers are also able to contribute to the platform, e.g., by providing justification of the apps' behaviour. The whole approach results in the assessment of mobile apps along two different metrics, which quantify their privacy-related behaviour, as judged by the users' contributions. To enhance participation and provide motivation for active contribution to the platform, we apply a unified rewarding strategy that includes gamification features for active users and developers. Note that CAP-A is not a technical solution, and does not scan or monitor users' devices or apps to assess their behaviour; instead, the project leverages crowdsourcing methods to improve user awareness [3].

## 2. The CAP-A tools

Due to space restrictions, we only describe the most important functionalities of the CAP-A tools, which are the following:

- *Expressing expectations* regarding the expected (or desired) privacy behaviour of each app (Subsection 2.1).
- *Annotating parts of a PrP document* in order to support other users in understanding its content (Subsection 2.2).
- *Accessing app privacy information*, including its privacy evaluation ratings, and viewing interesting statistics through the *Privacy Dashboard* (Subsection 2.3).
- The above functionalities are supported by a rewarding mechanism (Subsection 2.4), which aims at motivating the community to generate the necessary input.

We should note that the CAP-A tools include a mobile app, available through Google Play, which provides a mobile-friendly version of these functionalities. Moreover, developers are also part of CAP-A, and can claim the development of a certain app, giving them special privileges over that app, e.g., being able to justify the access requests of their apps. Details on these functionalities are omitted due to space limitations. The CAP-A tools can be found at: `https://www.cap-a.eu/tools`. Note that the CAP-A tools fully support both the English and the Greek language.

### *2.1. Expressing expectations*

Mobile apps often request access to specific parts of a mobile phone, such as the contacts, the camera etc. The CAP-A tools allow users to express their *expectations* with regards to such requests, i.e., whether they consider reasonable (or not) for a given app to make a given request, showing also the expectations of other users (see Figure 1 as an example).

[3] `https://cap-a.eu/`

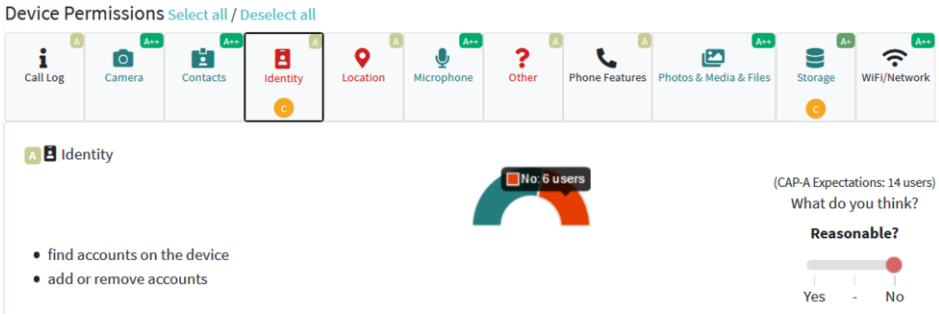


**Figure 1.** Expressing privacy expectations in CAP-A

### 2.2. *Annotating PrP documents*

The *PrP Annotator* allows users to mark a block of text in a PrP document and state its relevance to a certain request for access. Annotations are meant to highlight the important blocks in a PrP document, and how they are related to access requests, thereby simplifying the task of understanding its content (see Figure 2). The credibility of this information is assessed based on the (dis)agreement of users' annotations.

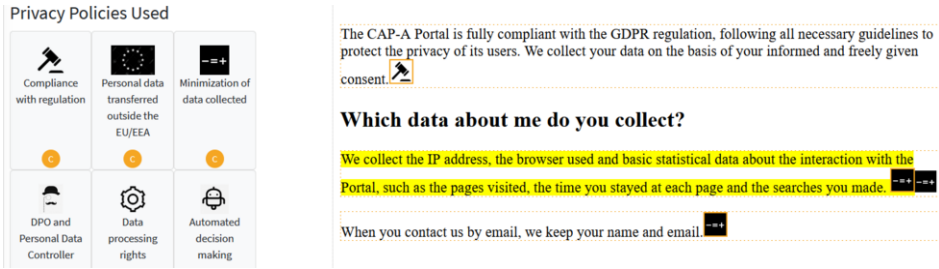


**Figure 2.** Annotating the PrP document of an app

### 2.3. *Privacy-related information on apps: Ratings, and the Privacy Dashboard*

Through CAP-A, users can access app-related information; apart from the standard information found also in Google Play, the user may be able to see privacy-related ratings for apps, namely the *"Satisfaction of Community's Expectations"* and the *"Privacy Friendliness"* ratings. The former is calculated based on how close the expectations expressed by the users are to what the application is requesting, whereas the latter takes into account privacy-related best practices, such as frequency of change and understandability of PrP documents, as assessed by users. The related calculations are based on a series of parameters that ensure an intuitive, as well as fair behaviour.

The *Privacy Dashboard* provides interesting visual representations of aggregated statistics regarding users and apps. More importantly, it provides an aggregation of users' input to allow the identification of patterns, such as specific preferences or stances of specific user groups towards certain app categories (e.g., see Figure 3). This can help developers understand how close their services are to what their clients would wish, or help policy makers and simple users identify trends. We constantly consider alternative diagrams to enrich the information given through the Privacy Dashboard.

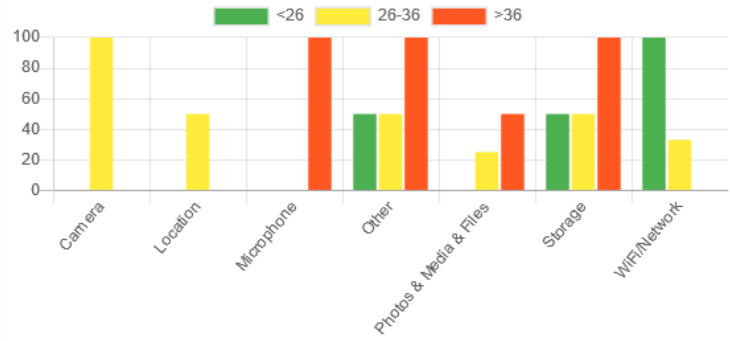


**Figure 3.** Privacy Dashboard: Game apps and reasonable access to permissions, based on user age

### *2.4. Rewarding mechanism*

Rewarding and gamification mechanisms are indispensable components of most crowd-based solutions. The rewarding mechanism of CAP-A is based on *tiers*, obtained through *points*, provided by *tasks* [2]. Tiers represent the experience level of a user in CAP-A (i.e., amount of interaction with the system). Points are earned through the accomplishment of tasks, which represent useful activities in the system and are organised in levels of sophistication; more complex ones are available to higher-tier users only, to avoid the probable ad-hoc behaviour of first-time users.

## 3. Conclusion

This paper presented the tools of CAP-A, which aim to improve privacy awareness and users' understanding of the privacy implications associated with the use of any given mobile app, based on crowdsourcing and collective intelligence measures. In our immediate future plans is the evaluation of our platform with real users, in the context of several planned pilots to take place throughout Europe, including a pilot involving legal experts for supporting the project from the legal perspective.

## Acknowledgement

This work has been supported by the EU H2020 programme under the NGI_TRUST grant agreement #825618.

## References

[1] Anton, A.I., Earp, J.B., Bolchini, D., He, Q., Jensen, C., Stufflebeam, W.: The lack of clarity in financial privacy policies and the need for standardization. In: IEEE Security and Privacy, vol. 2, (2004)

[2] Chrysakis, I., Flouris, G., Patkos, T., Dimou, A. and Verborgh, R. REWARD: Ontology for reward schemes. In $17^{th}$ Extended Semantic Web Conference: Posters and Demos, pp. 1-5 (2020).

[3] Chrysakis, I., Flouris, G., Ioannidis, G., Makridaki, M., Patkos, T., Roussakis, Y., Samaritakis, G., Stan, A., Tsampanaki., N., Tzortzakakis, E., Ymeralli., E.: Evaluating the data privacy of mobile applications through crowdsourcing. In $32^{rd}$JURIX 2020 (to appear).