A Rewarding Framework for Crowdsourcing to Increase Privacy Awareness

Ioannis Chrysakis, Giorgos Flouris, Maria Makridaki, Theodore Patkos, Yannis Roussakis, Georgios Samaritakis, Nikoleta Tsampanaki, Elias Tzortzakakis, Elisjana Ymeralli, Tom Seymoens, et al.

A Rewarding Framework for Crowdsourcing to Increase Privacy Awareness

Ioannis Chrysakis[1,3], Giorgos Flouris[1], Maria Makridaki[2], Theodore Patkos[1], Yannis Roussakis[1], Georgios Samaritakis[1], Nikoleta Tsampanaki[1], Elias Tzortzakakis[1], Elisjana Ymeralli[1], Tom Seymoens[4], Anastasia Dimou[3], and Ruben Verborgh[3]

[1] FORTH, Institute of Computer Science, Greece
{hrysakis,fgeo,patkos,rousakis,samarita,tsaban,ymeralli,tzortzak}@ics.forth.gr
[2] FORTH, PRAXI Network, Greece
{makridaki}@praxinetwork.gr
[3] IDLab, Department of Electronics and Information Systems, Ugent, imec, Belgium
{Ioannis.Chrysakis,Anastasia.Dimou,Ruben.Verborgh}@UGent.be
[4] imec-SMIT, Vrije Universiteit Brussel, Belgium
{Tom.Seymoens}@vub.be

Abstract. Digital applications typically describe their privacy policy in lengthy and vague documents (called PrPs), but these are rarely read by users, who remain unaware of privacy risks associated with the use of these digital applications. Thus, users need to become more aware of digital applications' policies and, thus, more confident about their choices. To raise privacy awareness, we implemented the CAP-A portal, a crowdsourcing platform which aggregates knowledge as extracted from PrP documents and motivates users in performing privacy-related tasks. The Rewarding Framework is one of the most critical components of the platform. It enhances user motivation and engagement by combining features from existing successful rewarding theories. In this work, we describe this Rewarding Framework, and show how it supports users to increase their privacy knowledge level by engaging them to perform privacy-related tasks, such as annotating PrP documents in a crowdsourcing environment. The proposed Rewarding Framework was validated by pilots ran in the frame of the European project CAP-A and by a user evaluation focused on its impact in terms of engagement and raising privacy awareness. The results show that the Rewarding Framework improves engagement and motivation, and increases users' privacy awareness.

Keywords: data privacy · privacy awareness · privacy policies · GDPR · crowdsourcing · rewarding · collective intelligence.

1 Introduction

Personal data is the hottest commodity in today's networked society [13,25]. On a daily basis, digital applications drive personal data use. These applications describe how they collect, control and process personal data in lengthy, vague

and frequently changing privacy policy documents (PrP) [4][1]. Thus, it is hard for users to read, understand and follow the updates of the PrP documents.

Privacy awareness reflects the extent to which a user is informed about privacy practices and policies, and about how disclosed information is used [39]. In other words, it reflects how clearly users understand the manner at which their data are handled and processed by used applications. Privacy awareness (i) helps users understand the privacy implications of using digital applications [20], e.g., when accepting permissions in device sensors (Camera, GPS); (ii) makes users more thoughtful in relevant situations [6], e.g., when downloading an application or giving their consent to a service provider; and (iii) contributes in counteracting the privacy paradox [33], i.e., the observation that although users are concerned about their privacy in real life, they act differently in their digital life [22]; indeed, we argue that the privacy paradox is due to limited awareness, so improved privacy awareness mitigates the problem.

Achieving privacy-awareness is difficult [36], but better results are achieved if users join forces through a crowdsourcing approach [17,14]. For example, in [32,38,7], crowdsourcing has been employed to allow users to annotate PrPs to clarify privacy practices, and thus improve their privacy knowledge. Also, crowdsourcing could allow users to evaluate the privacy friendliness of apps, e.g., by identifying GDPR concepts[2] in PrP texts, so they are better informed about the use of their personal data by applications [30,19].

One of the most fundamental challenges in crowdsourcing platforms is recruiting and engaging users [27]. Without engagement and motivation, user participation is significantly lower and the platform's objective is not achieved [18]. Combining intrinsic (fun, autonomy, reputation) and extrinsic (money, learning, forcedness, implicitness, task autonomy) rewards in crowdsourcing motivates users [24,40] and increases user participation and engagement.

This paper presents a *Rewarding Framework (RF)* for crowdsourcing activities, used in tandem with a crowdsourcing application to improve privacy awareness based on the crowd's collective knowledge. Such novel combination of crowdsourcing and rewarding to raise privacy awareness has not been considered so far. To design this framework, we identify basic characteristics, such as rewarding features, components and gamification principles, which motivate users, increase participation and achieve a sustainable solution that addresses the data privacy problem. The proposed RF model is based on REWARD [10], a general-purpose ontology designed to represent a reward strategy. The RF is adopted by the CAP-A portal[3], implemented and evaluated in the frame of the CAP-A European project[4], and supported by the established CAPrice Community[5].

[1] `https://www.varonis.com/blog/gdpr-privacy-policy/`
[2] `https://eur-lex.europa.eu/eli/reg/2016/679/oj`
[3] `https://www.cap-a.eu/portal`
[4] `https://www.cap-a.eu`
[5] `https://www.caprice-community.net`

2 Background and Related Work

In this section, we present related work on crowdsourcing with focus on privacy and existing gamification and rewarding features relevant to our approach.

2.1 Crowdsourcing and Privacy

By focusing on the problem of increasing data *privacy awareness* using crowdsourcing methods, we identify two main approaches enhanced by crowdsourcing: (i) *evaluation of applications* with respect to privacy based on user's opinion [1,2], and (ii) *annotation of Privacy Policy (PrP) documents* through participatory processes [32,38,7]. The former is highly relevant to ours as it focuses on mobile apps and use crowdsourcing tasks to monitor privacy goals. However, users' engagement is based exclusively on paid crowdsourcing activities (e.g., Mechanical Turk Human Intelligence Tasks[6]) and no other rewarding scheme, whereas ours is based on a combination of intrinsic and extrinsic rewards. In the latter, the design of crowdsourcing tasks is not straightforward due to privacy policies' vagueness. Users require more assistance and feedback to make successful contributions in privacy awareness. This needs to be considered when designing the crowdsourcing tasks included in the proposed Rewarding Framework (RF).

However, none of the aforementioned approaches applies a rewarding mechanism to maximize the crowd participation and improve the results. After all, the lack of participation and engagement is one of the most fundamental problems appearing in crowdsourcing [27]. Thus, ways to incentivize the crowd need to be identified, such as gamification schemes and rewarding methodologies. In this paper, we try to cover these needs by proposing a Rewarding Framework.

2.2 Gamification and Rewarding

Gamification refers to the application of game mechanics to a task that is not a game to increase user engagement, happiness or loyalty and constitutes a motivational driver to the success of a crowdsourcing technique [21]. McGonigal et. al. [27] suggests a generic gamification scheme based on four principles: *goal, rules, voluntary participation and feedback*. This scheme is suitable in crowdsourcing; hence we follow and extend it in our framework.

Several gamification features were proposed [28], such as *rewards, points and tiers*. Except from gamification principles and features, a gamification approach needs to be adjusted to the underlying crowdsourcing task's complexity [29]. Finnerty et. al. [16] evaluated task complexity in crowdsourcing, and showed that a clearer and simpler design, with less demand on workers' attention, provides more accurate results. For this reason, we considered the principle of flexible task management in the design of our proposed crowdsourcing privacy tasks.

[6] `https://www.mturk.com/`

In addition to gamification, *rewarding* the users strengthens the members' commitment and increases users' motivation to participate in, and contribute to, any crowdsourcing activity [3]. The positive impact of rewards to encourage participation in open source communities or citizen science initiatives has been well-documented in the related literature [23,31].

Scekic et. al. [35] identified different incentive mechanisms in different business environments used for social computing and crowdsourcing. The most relevant to our approach is the *Quota Systems and Discretionary Bonuses mechanism* [35]. In this mechanism, a number of performance metrics is set; when workers reach a threshold they earn a bonus. This is closer to the proposed RF, because users are rewarded according to their contributions and successful accomplishment of privacy-related crowdsourcing tasks.

3 The Rewarding Framework (RF)

First of all, in this section we present the relationship between CAP-A portal and RF. Then we describe the methodology that we used to design the RF. We analyze the critical rewarding features and rewarding components adopted by the RF, along with the gamification principles that we followed.

About the CAP-A portal. The Rewarding Framework (RF) was implemented as a fundamental component of the CAP-A portal, a crowdsourcing platform aiming to raise privacy awareness in mobile applications [12,11]. In CAP-A portal we applied the proposed rewarding features and components of the RF to reward users' contribution in crowdsourcing privacy tasks. The CAP-A portal is available at: `https://www.cap-a.eu/portal`

Methodology. Our framework (Figure 1) is based on existing works that fit well with the crowdsourcing paradigm. The RF design included the identification of the most appropriate **rewarding features** from existing approaches [41,26,28] that fit well with the crowdsourcing paradigm. The final result is a mix of *platform and user-centric methodology* [40]: a platform for aggregating privacy-related information from several users, announcing results, promoting new crowdsourcing activities etc., and dedicated tasks for users, according to their expertise and preferences.

Before starting designing any Rewarding Framework, the audience needs to be defined. In our case, both users of digital products/services and developers or companies that offer these services are considered. However, the proposed RF is addressed to users only, so we focus on *user-related tasks and features*.

We described the **rewarding features** in a conceptual model and evaluated it through several competency questions [10]. We implemented the RF's conceptual model as an ontology, the REWARD ontology[7], because an ontology gives us flexibility in the design, e.g., agile adaptation of rewarding features

[7] `http://www.w3id.org/reward-ontology`

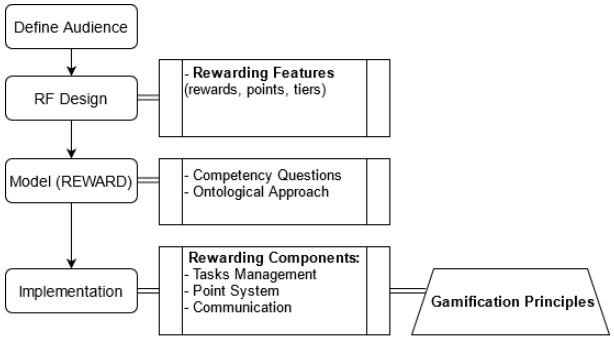


Fig. 1. The Reward Framework's design process

and components. We considered critical **rewarding components** (e.g., Communication, Point System) according to state of the art rewarding approaches. Finally, we adapted **gamification principles** in our approach to contribute to the further engagement of users in executing privacy tasks. We analyze below the aforementioned elements that we adopted in RF: rewarding features, rewarding components and gamification principles.

Table 1. Privacy tasks that lead to rewarding

Task Description	**Task Level**
Complete user profile	1
Share installed applications through the CAP-A app	1
Declare favorite applications	1
Download and login to the CAP-A app	1
Claim and acquire ownership of an app	1
Add a privacy expectation/justification	2
Add a URL evidence	2
Vote on the credibility of a given URL	2
Edit/Create annotations on PrP documents	3
Identify GDPR aspects	4

Rewarding Features. Our RF considers the following rewarding features: (i) **rewards**. We support both *intrinsic and extrinsic rewards* [21]. Intrinsic rewards are based on motivation that arises from within the individual, because it is naturally satisfying. Intrinsic rewards can be gained in RF through community interaction and participation in crowdsourcing tasks include learning, improving

skills in data privacy, achieving social recognition, self efficacy, entertainment through playful tasks and knowledge exchange.

Extrinsic rewards are based on motivation from actual material prizes, such as money, gifts, discounts etc. This type of motivation arises from outside the individual, as opposed to intrinsic motivation, which originates from inside of the individual. We support two types of extrinsic rewards, badges and leaderboards in RF. *Badges*, are special characterisations that a user gains when specific conditions (rules) are satisfied for this user (for details see the Appendix). The badges offer recognition in the community and allow participating in high-level crowdsourcing tasks, suggesting new ones, and having a more active role in the CAP-A portal. *Leaderboards* like in other similar approaches, are used to further motivate users [28]. They are a dedicated space in the CAP-A Portal that shows users with the highest points and applications with the highest ratings.

(ii) **points**. Our rewarding strategy was inspired by the *"Pay Per Performance"* and *"Quota Systems and Discretionary Bonuses"* [35] mechanisms. Thus, each user is rewarded with points for each completed task. The collection of points leads to the redemption of specified rewards which merit a pre-specified number of points. This policy motivates users to increase their privacy knowledge through the execution of privacy-tasks (table 1), while the whole community benefits from the resulting aggregated knowledge.

(iii) **tiers**. As in many successful reputation point systems [41], earned points are used to rank users ranked into one of the following tiers: *Baby, Novice, Grown-Up, Enthusiast, Warrior, Expert, Guru, Royal*[8] (see details on the Appendix, Table 5). Tiers help in keeping crowd workers in the loop and motivating them to always try to accomplish new tasks [41].

Rewarding Components and Implementation. Our aim is to support simple and flexible tasks for users. This **Task Management** policy allows users to select the crowdsourcing tasks that best match their needs and, thus, it has positive effects for both users and the community [16]. Thus in RF, tasks are available to users based on their credentials and tier, as well as the tasks' difficulty. To determine which tasks are available to which user, we identified four *task levels* to facilitate task management, each of them representing a different level of difficulty and sophistication:

- **Task Level 1**: tasks that do not demand much effort or expertise;
- **Task Level 2**: tasks related to other users;
- **Task Level 3**: time-consuming and sophisticated tasks that possibly contain a lot of transactions and iterations, or that were initiated by other users;
- **Task Level 4**: high-quality tasks that need to be verified by a system admin.

Higher-level tasks are initially locked and available only to users of higher-level tiers. This policy ensures high-quality feedback, avoiding the probable ad-hoc behaviour of first-time users. Each task follows the rules applied in each

[8] `https://cap-a.eu/portal#info`

respective level, which denote the amount of points for each task level according to the point system, and the task's availability according to the user tier (see Appendix, table 4).

Our RF includes a **Point System** to determine the details of the process of acquiring and redeeming points with rewards of the user's choice [41], following the practice of most rewarding systems where user tasks are associated with points [41]. The policy of the Point System ensures justice among users which comes from the equity theory: equity theory states that "people compare the ratios of their perceived outcomes to their inputs with the corresponding ratios of others"[34]. Due to lack of space we omit details regarding the Point System.

The **Communication** of the users' accomplishments and associated benefits contributes further to their engagement to the platform [28]. In our case, the Communication of results is performed through a specific notification mechanism, which informs users about their progress in the CAP-A portal (e.g, completed tasks, acquired points or other details with regards to the applied Point System). This mechanism also suggests steps for participating in more privacy tasks (and levelling-up), and announces the available rewards.

Gamification Principles Our RF and its features (e.g., points, badges, leaderboards, tiers, etc.) are heavily influenced by existing common gamification theories. Gamification plays a critical role in any rewarding strategy, as it results to a more fruitful process.

We apply the generic approach of McGonigal et. al.[27] which denotes that a gamification scheme should be based on: *common goal, rules of the game, feedback and voluntary participation.* In our case the *common goal* is raising privacy awareness. We extend this approach by setting as well *personal goals* for users following the expectancy theory [37]. This design option creates a wide gamification space for users and a clear relationship between tasks and rewards to contribute further to user's motivation.

Specifically, in the RF, gamification is supported by providing the following goals, which can be picked up by CAP-A users:

1. Level-up through community experience
2. Be included in the top20 list
3. Acquire knowledge on one's favourite applications
4. Express privacy concerns
5. Participate in the evaluation of applications
6. Improve the market towards building more transparent and privacy friendly applications

In our case the *rules of the game* are related to the accomplishment of tasks that cover several aspects of privacy focusing on PrP documents and are applied throughout the system.

Feedback is also a fundamental characteristic, because it makes goal achievement more realistic by showing gradual improvement and motivates users to

participate further [21]. Thus, the CAP-A portal gives *feedback* in several milestones for the accomplishment of tasks, in tiers level ups, earning of badges, rewards availability and redemption.

Finally, voluntary participation requires that everyone who is participating knowingly and willingly accepts the goals, the rules, and the feedback [27]. For this reason, we pursue a transparent policy to users, so that they can clearly denote their goals, and understand the gamification rules and the offering feedback of the CAP-A portal (e.g., through supporting users' history, denoting next steps for rewarding).

4 Validation

The Rewarding Framework (RF) was validated through six pilots focused on specific app categories and ran in the frame of the CAP-A project (see Table 2). Each Pilot followed a pre-designed workflow scenario, including requests to perform crowdsourcing actions that lead to rewarding. In total, 108 users participated in the pilots and 141 users registered to the CAP-A portal.

Pilot Name	**Duration**	**Participants**	**Apps Category**
Saferinternet4Kids	1/10 - 31/10	35	Games, Social Media & Communication
Bora	16/10 - 9/11	36	Business
REN	23/11 - 30/11	11	Conferencing
Devstaff	10/12 (Live)	8	Social media, Productivity
Praxi	16/12 - 23/12	5	Conferencing
Homodigitalis	15/10 - 15/12	13	all above categories

Table 2. CAP-A Pilots overview

The CAP-A portal allows two main types of interaction with the user, both of which are included in the RF and give points to users upon successful completion: expressing privacy expectations, and adding annotations on PrP documents. Both activities were included in the pilot scenarios, and resulted in meaningful contributions in terms of populating our privacy repository with user expectations and annotations; analysing these contributions is out of the scope of the current paper, but the interested reader is referred to the CAP-A portal statistics (`https://cap-a.eu/portal/#stats`) for details.

Our validation showed that the CAP-A portal and the RF worked properly without facing any problems; moreover, useful feedback for further improvement was received, which was organised in three main categories, analysed below.

Overriding the default behavior of RF. During the pilots, the RF's default behaviour should be overridden in some cases for promotion and motivation

purposes (e.g., to increase the points per task for a specific task and for a limited time period). Thus, the rewarding system should be flexible, parameterisable and adaptable. The implementation of our RF as an ontology helped us to easily address this demand; we added a *Boost Parameter* to the RF to support manual point adjustment. For example, the task of completing the user profile, important for the CAP-A portal's dashboard, was promoted for some of the last pilots.

Users info - history of activities. Users should be able to see their history of activities, e.g., for rewarding tasks. This functionality could help users monitor their past activities, and be further engaged in performing similar activities. This feature is related to the offered *"Feedback"* which is provided by the system to the users with regards to their accomplishments, and is a critical feature of reward systems [21,28]. To support this, we implemented in the CAP-A portal a *User's History* page, to clearly display past activities as a personal record dashboard.

UX improvement suggestions with regards to RF. During the pilots, it was clear that more information about the steps that a user should follow to level-up tier was needed. We concluded that an interface encouraging a more streamlined process would help users enjoy flexible navigation through the available tasks. This idea was implemented by redesigning the homepage of the CAP-A (to present alternative privacy tasks associated with the RF in a specific order).

5 Empirical Evaluation

After improving the CAP-A portal and the Reward Framework (RF) based on the feedback we received in the validation, we further performed an empirical evaluation with 11 participants who followed a specific workflow scenario [9]. The goal was to make a first assessment of how the system improvements can affect user engagement and privacy awareness. Our evaluation is an *exploratory study*, aimed at identifying critical success aspects of the RF and potential barriers or features that need to be further explored.

We considered both *objective* and *subjective metrics*. We evaluated engagement features, e.g., number of accomplished tasks compared to requested ones (objective metric), or users' opinion on the used features, e.g., points and tiers (subjective metric). We also evaluated privacy awareness with the *Privacy Awareness Index* [15], which measures the increase of privacy knowledge (objective) and the users' opinion on the acquired privacy knowledge (subjective).

We present below the *research questions (RQ)* and *hypotheses (H)* used to assess our targeted evaluation goals, as well as the evaluation setup, the methodology we followed to assess the impact of the RF, and the results of our study.

5.1 Research Questions and Hypotheses

We evaluated the impact of the RF along two dimensions: engagement of users, and raising of privacy awareness. Each dimension constitutes a different part in

our evaluation. We also made a UX evaluation to ensure that the user interface is not affecting negatively our results regarding user engagement and privacy awareness.

Part 1. Engagement and Motivation. We assess engagement and motivation indicators of the RF based on the following research questions and hypotheses:

- RQ1.1: *Are the users engaged while participating in crowdsourcing activities (as enabled by the CAP-A portal) due to the RF?*
  H1.1: *Users' engagement and participation is increased because of the RF.*
- RQ1.2: *Does rewarding encourage the participation level of users in participating in privacy related tasks requiring interaction?*
  H1.2: *Users are motivated to participate in actions requiring their feedback due to the RF.*
- RQ1.3: *Does rewarding affect positively the performance of users in executing privacy-related tasks?*
  H1.3: *Users gaining rewards are strongly motivated to perform more crowdsourcing privacy tasks.*
- RQ1.4: *Does rewarding affect users' return in the portal?*
  H1.4: *Rewarding makes users willing to return to the portal to perform additional crowdsourcing activities.*

To validate the above hypotheses, we asked a set of questions [8] to capture users' opinion (subjective metrics). We also used objective metrics extracted from the users' interaction with the portal. For example, to validate the most generic hypothesis H1.1, we examined the *response rate of participation* in specific crowdsourcing tasks of the workflow [9], and the *total number of accepted invitations* to register to the CAP-A portal. We also considered metrics indicating the users' actual engagement with the portal, e.g., the actual users' *interaction with the invited apps* and *their total points*, which gives a sense of the amount of work performed, in addition to the work required by the workflow scenario.

Finally, additional metrics were used to measure the level of engagement in the defined scenarios: *number of declared expectations*, *number of favorite apps*, *number of annotations in PrP documents*, and *number of total examined apps.*

Part 2. Privacy Awareness. Common privacy awareness questions were asked before and after the use of the CAP-A portal to assess whether privacy awareness increased. Similarly to Part 1, we formulated a set of research questions and hypotheses to evaluate privacy awareness [8]:

- RQ2.1: *Does participation in the CAP-A portal improve privacy awareness?*
  H2.1: *Users who used the CAP-A portal improved their privacy awareness.*
- RQ2.2: *Does the RF have a positive impact in raising privacy awareness?*
  H2.2: *Users with less experience in rewarding tasks (low amount of points) are less privacy-aware.*

- RQ2.3: *Does the tier level up affect the increased privacy awareness of users?*
  H2.3: *Users that level-up tier increase their knowledge on privacy.*
- RQ2.4: *Does the RF encourage users to make privacy aware actions through the portal?*
  H2.4: *The RF motivates users to offer their privacy expectations, to improve the community's privacy awareness.*

5.2 Evaluation Setup

For the evaluation setup, following the approach of [15], we define the following elements: participant details, the goals of the evaluation, the applied methodology, and the final expected results.

Participant Details. For our evaluation process, we invited 15 participants from two different countries. The participants belonged to three different age groups and had different background and level of knowledge with respect to technology, mobile apps and privacy. By calculating the users' *Privacy Concerns Index* (PCI), following the approach of [5] we classified them into three categories to check the impact of the RF to different categories of users (see Users Classification subsection). All users who participated download and install mobile applications that handle their personal data, so it is interesting for them to learn more about their data utilization by service providers and developers.

Evaluation Goals. The goal of the evaluation is twofold: (i) assess the impact of the proposed RF in the engagement and motivation of users to participate in privacy related tasks; and, (ii) improve users' privacy awareness due to their participation in a crowdsourcing approach that applies this RF.

Evaluation Methodology. For our evaluation, we combined a Survey Part with an Experimental Part following [5].

The *Survey Part* aims to collect the participants' demographic characteristics, estimate their privacy concerns, and classify their concerns into different categories according to their common interests and acquired knowledge with regards to privacy. It consists of a *Pre-Questionaire* where we use the popular Likert scaling[9], as it is equidistant and well elaborated. After applying the Pre-Questionaire to the target audiences, *Pre-Activities* are used to explain the evaluation process of the experimental part, whereas *Post-Activities* are used to correlate the results from the experimental part (objective) with answers to subjective related questions for both engagement and awareness.

The Pre-Activities include a Pre-Questionaire to capture *Demographic* and *Background* information for users and calculate the *Privacy Concerns Index (PCI)* to classify them to different categories following the approach of [5].

[9] `https://conjointly.com/kb/likert-scaling/`

The Post-Activities include a Post-Questionnaire to evaluate the success of the engagement and motivation strategy (Part 1), and privacy awareness methods used (Part 2), according to the evaluation's goals. To ensure that the applied User Interface does not get in the way of the goal of improving privacy awareness, we validated some common usability metrics[10] through a UX Questionaire, namely, *user's subjective satisfaction, success rate*, and *required time*.

The *Experimental Part* aims to assess the impact on users' behavior while interacting with the RF. It consists of a specific workflow scenario [9], in which we evaluate a set of parameters regarding user engagement and improvement of privacy awareness through interaction with the CAP-A portal and the applied RF. This part is also correlated with the respective Post-Questionnaire which is collected after this interaction to draw conclusions about user engagement and motivation and their level of privacy awareness.

Expected Results. Our expected results include:

1. a *users classification* according to their background and privacy expertise based on the Pre-Questionnaire;
2. insights about *user engagement and motivation* and comparisons on quantitative metrics that resulted from the user interaction with the RF;
3. insights regarding the RF impact on users' *privacy awareness level*;
4. *Correlation of results* of the Pre- and Post-Questionnaire.

5.3 Results

We present the users classification, results and conclusions for our evaluation.

Users Classification 11 participants fulfilled the evaluation. Following the approach of [5], the categories and the respective classifications for users were:

- **Fundamentalists**, users really sensitive to privacy with high privacy concerns); 5 of our users were classified as fundamentalists.
- **Pragmatists**, users that care for privacy; 3 of our users were classified as pragmatists.
- **Unconcerned**, users that do not really have special concerns with regards to privacy; 3 of our users were classified as unconcerned.

Part 1. Engagement and Motivation. In total, 73% of users actively participated in the evaluation. We considered as active any user who was invited, registered to the CAP-A portal and completed at least one rewarding task of the defined scenario. Interestingly, most users have not participated in any privacy-awareness activity in the past according to the replies in the Pre-Questionaire, and still accepted to participate in such a privacy activity; as a result, engaging them to the related crowdsourcing task becomes more challenging.

[10] `https://www.nngroup.com/articles/usability-metrics/`

In the majority of the cases, and for all types of users, the participation rate exceeded the minimum number of 10 tasks specified in the scenario [9], revealing high engagement to the CAP-A portal. Each user accomplished on average 41 tasks, 13.5 tasks per user if we consider unique actions per app (table 3).

Table 3. Completed tasks per user

User	Expectations (min 3)	Favorites (min 5)	Annotations (min 1)	Examined Apps (min 5)
User 1 (F)	30	5	0	5
User 2 (P)	18	8	3	8
User 3 (P)	3	5	1	5
User 4 (F)	53	8	3	8
User 5 (F)	30	5	0	5
User 6 (U)	24	9	4	10
User 7 (F)	28	5	0	7
User 8 (F)	49	5	2	5
User 9 (P)	41	5	1	5
User 10 (U)	26	8	2	8
User 11 (U)	42	20	1	22

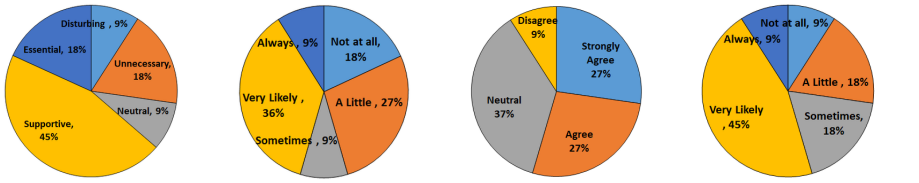
(F): Fundamentalist; (P): Pragmatist; (U) unconcerned

Comparing these results, i.e. response rate of participation in completed tasks, with results of the *subjective* questions in Part 1 of the Post-Questionnaire (to validate research questions RQ1.1, RQ1.2 and RQ1.3), we can clearly draw positive results regarding user engagement. Specifically, most users agreed that the RF positively affects their activities in the CAP-A portal (Figure 2(b)).

In addition, it seems that the RF motivates users in participating in privacy tasks requiring their interaction: 54% of the users agreed with this, 37% appeared neutral and only 9% disagreed (Figure 2(c)). This argument is reinforced by the fact that the task that most users completed is the expression of expectations (Table 3). Thus, users preferred to express expectations than adding favorites which is a naive task. Thus, the interaction of users through participation in privacy tasks ultimately helps to improve their privacy knowledge. The applied rewarding features (e.g., points and tiers) motivates 72% of the users, namely user engagement is achieved through interaction with the RF (Figure 2(d)).

More than half of the users had positive or neutral impression for the RF (72%). Specifically, 45% of users think that the RF is supportive and 18% believe it is essential, 9% are neutral, 18% think it is unnecessary and only 9% think that is disturbing. The results are displayed graphically in Figure 2(a).

We further examined the users who appeared negative (1 user) or neutral (2 users). We noticed that these users performed 40, 40 and 52 tasks respectively, which is much more than the minimum total requested number of tasks (10 tasks). However, we also found that 2 of them did not participate in the



(a) How did users experience the RF?

(b) Does rewarding affect users activity in the CAP-A portal?

(c) The RF triggers users in tasks that require their feedback

(d) How much RF features motivate users to participate in more activities?

Fig. 2. Evaluating users' engagement and motivation

annotation task. For this reason we included a dedicated question regarding the ease of annotation task in the UX evaluation below.

According to their replies in the Post-Questionnaire, 64% of users spent more than 10 minutes in the CAP-A portal, which is much more than the estimated 5 minutes necessary to complete the scenario. This shows engagement, and clearly demonstrates that the RF increases users' return to the portal (RQ 1.4).

Part 2. Privacy Awareness. In the second part of our evaluation, we compared the Privacy Awareness Index (PAI) for the same users before and after the execution of the workflow scenario. This experiment mainly assessed the research questions RQ2.1, RQ2.2 and RQ2.3. Our results show a very high increase on the level of privacy awareness for all users and all categories (the highest increase, 500%, appeared in User 9(P), see Figure 3). For Unconcerned and Pragmatist users the increase was 288% and 286% on average, while for Fundamentalists we noticed a 151% increase. We also noticed a significant improvement in the level of privacy awareness for users who have children (246%). Thus, it is very encouraging that this category of users who were classified as the most unconcerned, exhibited considerable increase in their privacy awareness index.

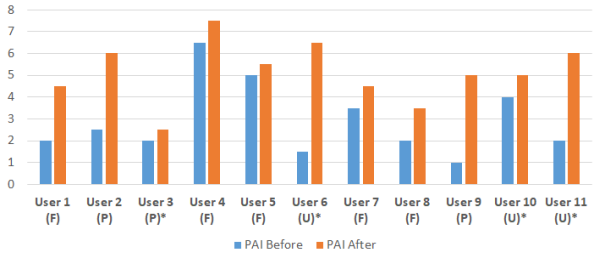
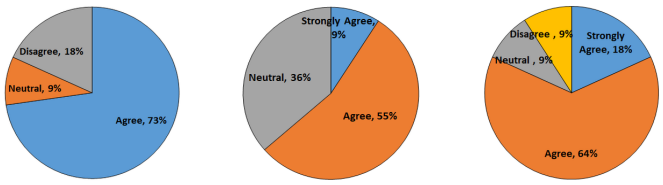


Fig. 3. Privacy Awareness Index (PAI), max:8, users who have kids marked with a star



(a) Users likely to participate in future privacy tasks

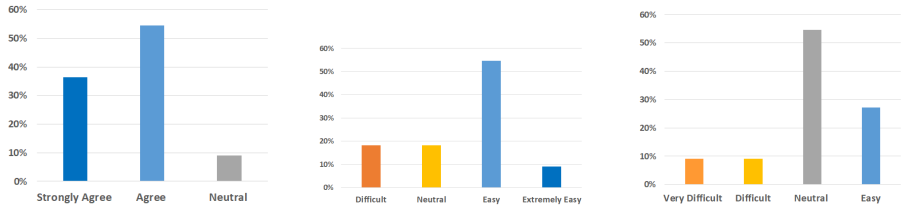
(b) Users express their privacy contributions

(c) Users are aware of personal data handling

Fig. 4. Evaluating privacy awareness

Furthermore, the RF proved that it motivates users to contribute in privacy awareness actions through the CAP-A portal (RQ 2.4). This conclusion is drawn since most users (73%) agree that it is very possible to participate in a new privacy task in the future due to the RF (Figure 4(a)).

Most users (55%) agree that due to the RF, they make their own privacy contributions such as expressing privacy expectations on device permissions (see figure 4(b)). The interaction of users with the RF helps them to become aware and knowledgeable about how personal data are handled by mobile applications and service providers; 82% of participants agreed with this claim (Figure 4(c)).



(a) RF well described and clearly noticeable

(b) Easiness to perform a task in CAP-A portal

(c) UX and ease of annotation task

Fig. 5. UX evaluation

UX Evaluation. Users did not experience any difficulty in understanding and identifying the main RF features. 91% agreed that the RF features (such as tasks, points and tiers) are well described, whereas 9% appeared neutral (Figure 5(a)). The results of our User Experience (UX) evaluation showed that the CAP-A portal interface offers an easy and straightforward way to perform the main privacy tasks related to the RF. 64% or users found easy or extremely easy to perform a task in the portal (Figure 5(b)). Adding annotations was the most difficult task: 9% of the users found it very difficult, 9% difficult, 55% neutral

and 27% easy (Figure 5(c)). Nevertheless, 5 out of 11 users completed more than the minimum requested annotations (Table 3). This shows that, although the interface of the Annotator tool was not an obstacle, it still has room for improvement to offer a more attractive way of annotating PrP documents.

6 Conclusion and Discussion

In this paper, we propose a Rewarding Framework (RF), which was applied in the CAP-A crowdsourcing platform as a tool for raising privacy awareness. The validation and evaluation of the RF led to some interesting empirical findings, showed promising results regarding user engagement, and contributed in improving users' privacy awareness. To the best of our knowledge, rewarding has not been evaluated so far to raise privacy awareness.

Our study showed that it is very important for a rewarding framework to be agile (in terms of overriding its default behavior), supporting fair rewards according to the complexity of each task, and providing a transparent mechanism of offering feedback to users (showing their progress in personal goals, or how their contributions make an impact towards the common goal of the community).

It is also important for rewarding frameworks to provide an easy way to achieve initial goals, so that new users are not repelled. Equally important is to utilize appropriate terminology to refer to the RF features, such as the experience points earned or the achievements accomplished, so that the users feel that they are becoming domain experts, in some sense, as they become more involved.

In addition, dealing with annotating PrP documents and extracting privacy-related information from them, proved to be a hard task for some users. Thus, we should further examine how to provide an enhanced User Experience with regards to this task, by appropriately adjusting the RF to further promote the annotation task, e.g., by giving more points for completing it, or by creating an appropriate badge for users that are returning to the annotation task.

Our future plans include a new round of user evaluation, focusing on specific rewarding components (e.g., point system), different user types (e.g., developers) and employing a larger number of users. Our intention is to further improve our approach based on the feedback, in order to optimise our RF and use it to help sustain a community of privacy-aware citizens in the context of CAP-A.

Acknowledgement

This work has been supported by the CAP-A project which has received funding from the European Union's Horizon 2020 research and innovation programme under the NGI_TRUST grant agreement no 825618. The described research activities were also funded by Ghent University, imec, Flanders Innovation & Entrepreneurship (VLAIO). Ruben Verborgh is a postdoctoral fellow of the Research Foundation – Flanders (FWO).

References

1. Amini, S., Lin, J., Hong, J.I., Lindqvist, J., Zhang, J.: Mobile application evaluation using automation and crowdsourcing (2018). https://doi.org/https://doi.org/10.1184/R1/6470255.v1
2. Amini, S.: Analyzing mobile app privacy using computation and crowdsourcing. Ph.D. thesis, Carnegie Mellon University (2014)
3. Antikainen, M.J., Vaataja, H.K.: Rewarding in open innovation communities–how to motivate members. International Journal of Entrepreneurship and Innovation Management **11**(4), 440–456 (2010)
4. Antón, A.I., Earp, J.B., He, Q., Stufflebeam, W., Bolchini, D., Jensen, C.: Financial privacy policies and the need for standardization. IEEE Security & privacy **2**(2), 36–45 (2004)
5. Bergmann, M.: Testing privacy awareness. In: IFIP Summer School on the Future of Identity in the Information Society. pp. 237–253 (2008)
6. Bergram, K., Bezençon, V., Maingot, P., Gjerlufsen, T., Holzer, A.: Digital nudges for privacy awareness: From consent to informed consent? In: ECIS (2020)
7. Bhatia, J., Breaux, T.D., Schaub, F.: Mining privacy goals from privacy policies using hybridized task recomposition. ACM TOSEM **25**(3) (2016)
8. Chrysakis, I.: CAP-A rewarding framework evaluation - list of questions (2020). https://doi.org/10.6084/m9.figshare.13042772.v8
9. Chrysakis, I.: Introduction to CAP-A portal & rewarding evaluation scenario (2020). https://doi.org/10.6084/m9.figshare.13042787.v5
10. Chrysakis, I., Flouris, G., Patkos, T., Dimou, A., Verborgh, R.: REWARD: Ontology for reward schemes. In: ESWC 2020. pp. 55–60. Springer (2020)
11. Chrysakis, I., Flouris, G., Ioannidis, G., Makridaki, M., Patkos, T., Roussakis, Y., Samaritakis, G., Stan, A., Tsampanaki, N., Tzortzakakis, E., Ymeralli, E.: CAP-A: a suite of tools for data privacy evaluation of mobile applications. In: JURIX (2020)
12. 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: JURIX (2020)
13. Craig, T., Ludloff, M.E.: Privacy and big data: the players, regulators, and stakeholders. O'Reilly Media, Inc. (2011)
14. Diamantopoulou, V., Androutsopoulou, A., Gritzalis, S., Charalabidis, Y.: An assessment of privacy preservation in crowdsourcing approaches: Towards GDPR compliance. In: RCIS. pp. 1–9. IEEE (2018)
15. Fatima, R., Yasin, A., Liu, L., Wang, J., Afzal, W., Yasin, A.: Sharing information online rationally: An observation of user privacy concerns and awareness using serious game. Journal of Information Security and Applications **48** (2019)
16. Finnerty, A., Kucherbaev, P., Tranquillini, S., Convertino, G.: Keep it simple: Reward and task design in crowdsourcing. In: CHItaly (2013)
17. Flouris, G., Patkos, T., Chrysakis, I., Konstantinou, I., Nikolov, N., Papadakos, P., Pitt, J., Roman, D., Stan, A., Zeginis, C.: Towards a collective awareness platform for privacy concerns and expectations. In: ODBASE (2018)
18. Grobbink, E., Peach, K.: Combining crowds and machines (2020), `https://www.nesta.org.uk/report/combining-crowds-and-machines/`
19. Hatamian, M., Kitkowska, A., Korunovska, J., Kirrane, S.: 'It's shocking!': Analysing the impact and reactions to the A3: Android apps behaviour analyser. In: DBSec. pp. 198–215 (2018)

20. Kani-Zabihi, E., Helmhout, M.: Increasing service users' privacy awareness by introducing on-line interactive privacy features. In: Nordic Conference on Secure IT Systems. pp. 131–148. Springer (2011)
21. Kavaliova, M., Virjee, F., Maehle, N., Kleppe, I.A.: Crowdsourcing innovation and product development: Gamification as a motivational driver. Cogent Business & Management **3**(1) (2016)
22. Kokolakis, S.: Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & security **64** (2017)
23. Krishnamurthy, S., Ou, S., Tripathi, A.K.: Acceptance of monetary rewards in open source software development. Research Policy **43**(4) (2014)
24. Lee, T.Y., Dugan, C., Geyer, W., Ratchford, T., Rasmussen, J., Shami, N.S., Lupushor, S.: Experiments on motivational feedback for crowdsourced workers. In: 7^{th} AAAI Conference on Weblogs and Social Media (2013)
25. Liang, F., Yu, W., An, D., Yang, Q., Fu, X., Zhao, W.: A survey on big data market: Pricing, trading and protection. IEEE Access **6** (2018)
26. McCall, M., Voorhees, C.: The drivers of loyalty program success: An organizing framework and research agenda. Cornell Hospitality Quarterly **51**(1), 35–52 (2010)
27. McGonigal, J.: Reality is broken: Why games make us better and how they can change the world. Penguin (2011)
28. Morschheuser, B., Hamari, J., Koivisto, J.: Gamification in crowdsourcing: a review. In: 49^{th} Hawaii International Conference on System Sciences (2016)
29. Morschheuser, B., Hamari, J., Koivisto, J., Maedche, A.: Gamified crowdsourcing: Conceptualization, literature review, and future agenda. International Journal of Human-Computer Studies **106**, 26–43 (2017)
30. Nejad, N.M., Scerri, S., Lehmann, J.: KnIGHT: Mapping privacy policies to GDPR. In: European Knowledge Acquisition Workshop. pp. 258–272 (2018)
31. Newman, G., Wiggins, A., Crall, A., Graham, E., Newman, S., Crowston, K.: The future of citizen science: emerging technologies and shifting paradigms. Frontiers in Ecology and the Environment **10**(6) (2012)
32. Oltramari, A., Piraviperumal, D., Schaub, F., Wilson, S., Cherivirala, S., Norton, T.B., Russell, N.C., Story, P., Reidenberg, J., Sadeh, N.: Privonto: A semantic framework for the analysis of privacy policies. Semantic Web **9**(2), 185–203 (2018)
33. Pötzsch, S.: Privacy awareness: A means to solve the privacy paradox? In: IFIP FIDIS Summer School. pp. 226–236. Springer (2008)
34. Samaha, S.A., Palmatier, R.W., Dant, R.P.: Poisoning relationships: Perceived unfairness in channels of distribution. Journal of Marketing **75**(3), 99–117 (2011)
35. Scekic, O., Truong, H.L., Dustdar, S.: Incentives and rewarding in social computing. Communications of the ACM **56**(6), 72–82 (2013)
36. Solove, D.J.: The myth of the privacy paradox. Available at SSRN (2020)
37. Vroom, V.H.: Work and motivation. Wiley (1964)
38. Wilson, S., Schaub, F., Ramanath, R., Sadeh, N., Liu, F., Smith, N.A., Liu, F.: Crowdsourcing annotations for websites' privacy policies: Can it really work? In: Proceedings of WWW-16. pp. 133–143 (2016)
39. Xu, H., Dinev, T., Smith, H.J., Hart, P.J.: Examining the formation of individual's privacy concerns: Toward an integrative view. In: ICIS (2008)
40. Yang, D., Xue, G., Fang, X., Tang, J.: Crowdsourcing to smartphones: Incentive mechanism design for mobile phone sensing. In: MobiCom (2012)
41. Zichermann, G., Cunningham, C.: Gamification by design: Implementing game mechanics in web and mobile apps. O'Reilly Media, Inc. (2011)

Appendix: RF Implementation details

We present below details regarding the rules that we applied for task levels, tiers and for the introduced badges in the RF implementation.

Table 4. Task Levels

Task Level	**Earned Points**	**Tier Availability**
1	$W_1 * C$ Points ($W_1 = 1$)	Baby to Royal
2	$W_2 * C$ Points ($W_2 = 1$)	Novice to Royal
3	$W_3 * C$ Points ($W_3 = 2$)	Grown-Up to Royal
4	$W_4 * C$ Points ($W_4 = 4$)	Expert to Royal

TaskLevelAdjustmentParameter = W_i for $i > 0$ and
$i \leq$ Task Levels Number, C = MinTaskLevelThreshold in points

Table 5. Available Tiers

Tier	**Required Points**
Baby	Zero points
Novice	$V_1 * D$ Points ($V_1 = 5$)
Grown-Up	$V_2 * D$ Points ($V_2 = 15$)
Enthusiast	$V_3 * D$ Points ($V_3 = 20$) points
Warrior	$V_4 * D$ Points ($V_4 = 50$) points
Expert	$V_5 * D$ Points ($V_5 = 100$)points
Guru	$V_6 * D$ Points ($V_6 = 500$) points
Royal	$V_7 * D$ Points ($V_7 = 1000$) points

TierLevelAdjustmentParam = V_j for $j > 0$ and $j \leq$ Tiers Number
D = FirstTierThreshold in points

Badges

- **Social/Buddy**: users who invited more than five friends to join the system or to accomplish a specific task within a month;
- **Super Star**: users who completed at least ten tasks in a month;
- **On Fire**: users who completed more than three tasks in the last week;
- **Ambassador**: users with high expertise on various tasks or on privacy issues; ambassadors are invited/suggested by the crowd or by other ambassadors.
- **Inactive**: users who joined the system but did not start/complete any task;
- **Sleepy**: users who completed at least one task but did not start a new one for the last three months.