Keep System Status Visible: Impact of Notifications on the Perception of Personal Data Transparency

Lucia Vilela Leite Filgueiras[1(✉)], Adriano da Silva Ferreira Leal[1], Thiago Adriano Coleti[1,3], Marcelo Morandini[2], Pedro Luiz Pizzigatti Correa[1], and Solange N. Alves-Souza[1,3]

[1] Escola Politécnica, Universidade de São Paulo, São Paulo, SP, Brazil
lfilguei@usp.br
[2] Escola de Artes, Ciências e Humanidades, Universidade de São Paulo, São Paulo, SP, Brazil
[3] Centro de Ciências Tecnológicas, Universidade Estadual do Norte do Paraná, Jacarezinho, PR, Brazil

Abstract. Personal Data Transparency (PDT) requires that companies provide information for subjects about activities performed in their personal data such as collecting, processing, disseminating and sharing. Recent regulations on personal data have addressed the improvement of subjects' capability in giving consent to controllers/processors, ensuring that data collection and usage policies are presented to the subject in an intelligible and easily accessible form, using clear and plain language. However, the objective of ensuring that people have more control over their personal data presumes that they are conscious on the value of their personal data, understand the concept of privacy, and are aware of risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. This conscience should be complete in the moment of consent. Wisely, regulators have been cautious and included the right to withdraw the consent and the right of having personal data "forgotten". However, a person's conscience of risks comes with experience brought by the exposition to the facts, whether good or adverse, that happen after consent is given. Users frequently accept all terms without fully agreeing with them because they are motivated to access a service or product. In this paper, we report and discuss the results of an experiment showing that instantaneous notification of data collection to smartphone users' increases significantly their awareness of transparency. Based on this discussion, we advocate that feedback should be enforced in the transparency regulations.

Keywords: Feedback · Personal Data Transparency · Data Protection Regulation

1 Introduction

Data driven systems and services have boosted the need for data collection and data processing, whether proprietary or third-party data. Within collected data, personal data has a special importance both for controllers/processors (companies that collect and

M. Kurosu (Ed.): HCII 2019, LNCS 11568, pp. 513–529, 2019.
https://doi.org/10.1007/978-3-030-22636-7_39

process data) and for data subjects (owners of data). Personal data is any information relating to an identified or identifiable natural person [1] (European Union, 2016).

The interest in data produced by individuals or communities is so evident that it is currently unlikely that a digital service or application operates without collecting personal data or without using information produced through personal data.

Aspects of ethics regarding personal data have been receiving attention from the academic and professional communities in the new research area of Human-Data Interaction [2] (Mortier *et al.*, no date).

One of the biggest challenges in this area is the study of Personal Data Transparency (PDT). PDT occurs when the individuals affected by the data collection and processing are aware of the complete flow concerning their personal data, from collection, transformation, processing, to their availability and use - not by deduction or supposition, but because the flow is well documented and exposed in an intelligible way to the users of a certain service or product. In the past decade, the concerns about PDT became more significant due to the reason that the use of personal data also increased for several commercial and non-commercial reasons.

Recent regulations on personal data protection like European General Data Protection Regulation - GDPR [1] have improved clarity and understandability of privacy policies and usage terms and conditions are presented to the user. This regulation determines that service providers state how and when user data will be collected and used, warranting the users important rights (such as the right to be forgotten) and avoiding leakage of personal information to unauthorized companies.

Mortier and colleagues [2] associate the concepts of transparency and intelligibility to legibility. According to the authors, "(p)remised on the recognition that interactions with data flows and data processes are often opaque, legibility is concerned with making data and analytic algorithms both transparent and comprehensible to users." In this paper, we use the term legibility as a quality associated to the user's perception of transparency, that is, the degree with which a system, product or service communicates its transparency to their users.

It is interesting to notice that, according to Oliver [3], in the context of public policies and governance, the term transparency used to mean "letting the truth available for others to see if they so choose", that implies that observers of transparency may not want to look, or may not have the means to look, or may not have the ability to see the truth. In modern organizations and governments, this form of passive transparency is giving place to active disclosure, in which controllers have the responsibility of releasing clear and updated information to stakeholders so that they can manage risk effectively.

In fact, the motivation for this work stems from the observation that users of digital services may not want to look or may not have the means to look or may not have the ability to see the truth regarding their data. These users, from now on in this paper referred to as "data subjects", are often aware of data collection and processing, but they do not know when, how or where they happen, and they do not give due importance to examining terms of use and privacy policies of digital services before consenting.

Among other reasons for this careless behaviour is the fact that data subjects are requested to examine privacy policies and usage terms and conditions at the time they

are contracting a desired service and under the self-imposed pressure for beginning to use, with little or no power of negotiation.

Tasks performed upon personal data are often opaque for subjects, even though they may have a strong relationship with people's privacy, security and agency. Even though data subjects have the intellectual and legal ability to decide and to take risks, as with every new technology, the implications of personal data usage are yet to be discovered. In this situation, capable adults may be as a vulnerable as a child. Regulators have been wise to include the right to revoke the consent and the right of deletion of a person's data, given that many consequences of usage of personal data are not yet possible of identification.

One of the most relevant design rules for human-computer interaction is "visibility of system status". This rule is explained by Nielsen and Norman: "The system should always keep users informed about what is going on, through appropriate feedback within reasonable time." [4]. Visibility of system status requires the system to always give users prompt and unambiguous feedback so that they can diagnose the state the system is in and whether an action produced any changes in this state. Lack of visibility of system status has been a contributing factor in many industrial accidents in history and is still the cause of many usability problems in different systems, from critical systems [5] to wearables [6].

We show, in this paper, that instantaneous notification to a data subject of data collection can improve legibility. We advocate that requirements of feedback should be addressed and enforced because of its great potential to educate users towards conscious consent.

In order to discuss this issue, we organize the paper as follows. In Sect. 2, we present the concept of feedback and the heuristic of visibility of system status in the context of designing usable systems. In Sect. 3, we analyse GDPR to show how the regulation addresses legibility and feedback. In Sect. 4, we describe our active disclosure experiment to assess the impact of feedback on users' data collection on their perception of transparency. Section 5 details the results, based on which, in Sect. 6, we discuss how recent regulations should address users' awareness of personal data collection and propose changes in the regulation text to enforce the development of notifications.

2 Feedback and Visibility of System Status

Feedback is the reaction to a process/activity, or the information obtained from a given action. For HCI community, the term feedback means the communication of the result of any interaction and should be easily visible and understandable by humans.

According to Harley [7], communicating the current state of the system allows users to feel in control, take appropriate actions, and thus feel more confident. This communication or feedback contributes to transparency about system behaviour and results in better decision making. It's not hard to find simple, ordinary examples of feedback, such as the smartphone battery alert, warning of unread emails in your inbox, and even an elevator signalling your current floor. Harley further states that system state visibility refers to how well the current state of the system is passed on to users,

and ideally systems should always keep users informed of what is happening through feedback at an appropriate time.

Feedback can assume two forms regarding the time moment that it is issued. While final feedback signals the completion of a given activity and the change in system state, instantaneous feedback informs on the ongoing activities of a system. For instance, in a train control system, the operator could see a railroad switch icon as a blinking icon while the physical object is in movement between two stable states. In file transfers, the dynamic filling bar reports that the operation is being carried on. Both forms of feedback are important to keep users aware of system state.

Information on system status helps build users' trust in the system, because users can keep a mental model of the system logic thus anticipating consequences of their actions.

3 GDPR and Legibility

The General Data Protection Regulation (GDPR) was created to protect European citizens regarding the processing of personal data and to establish rules to provide a sound base for movement of personal data within the member states.

The initiative has promoted important changes in personal data collection and processing, by imposing measures of privacy and data protection. The text was published in the Official Journal of the European Union on May 4, 2016 and provided a two-year adaptation time. Since May 25, 2018, the regulation is effective in all member states. Regulation, as its name implies, dictates obligations of companies providing services on the processing of personal data and privacy of citizens of the European Union. Failure to comply with the rules imposes sanctions on companies, and fines may reach 4% of annual revenues up to 20 million euros if the violations are serious.

The regulation is organized in Chapters that address General provisions, Principles, Rights of the data subject, Controller and processor, Transfers of personal data to third countries or international organisations, Independent supervisory authorities, Cooperation and consistency, Provisions relating to specific processing situations, Delegated acts and implementing acts and Final provisions. The regulation has 99 articles and 173 recitals. A recital is part of the legal text that explains the context and purpose for many articles, disclosing how the regulation is interpreted by Data Protection Authorities.

GDPR grants subjects several rights regarding their personal data, from the right to request information on whether personal data concerning them are being processed to the right of being forgotten. In this work, we have scrutinized GDPR to capture the general understanding of transparency and legibility. Articles that address this matter are concentrated in the first three chapters the regulation and in some of its recitals. We group in the following paragraphs citations of the regulation that express provisions for subjects' awareness of their rights, even though the regulation has not as primary motivation to educate citizens on their rights but to protect these rights.

1. Consent must be informed. GDPR states that collection and processing personal data depend on data subjects giving consent for every purpose. Consent is a freely given affirmative action, either by a statement or by a clear action, that must be

specific to the purpose of processing. In order to consent be informed, GDPR requires that any information and communication relating to the processing of personal data must be easily accessible and easy to understand. Clear and plain language must be used to communicate.

2. Access request to controller information. In article 15, GDPR states the right of access by data subjects to obtain from the controller confirmation as to whether personal data concerning them are being processed, as well as:

   – the purposes of the processing;
   – the categories of personal data concerned;
   – the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
   – where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
   – the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
   – the right to lodge a complaint with a supervisory authority;
   – where the personal data are not collected from the data subject, any available information as to their source;
   – the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Details of processing operations and standardized icons. Recital 60 states that the data subject must be informed on details of processing operations and that standardized icons can be used to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing:

   – existence of the processing operation
   – its purposes
   – specific circumstances and context in which the personal data are processed
   – existence of profiling and the consequences of such profiling
   – whether the subject is obliged to provide the personal data and of the consequences, where he or she does not provide such data.

4. Agency regarding subjects' rights. Recital 59 states that controllers must provide **modalities** [emphasis added] for facilitating the exercise of the data subject's rights including mechanisms to request, obtain access to personal data, rectifying, erasing and objecting to processing. This statement improves the quality of agency of data subjects regarding their rights to manage their personal data.
5. Data subjects "should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing." (Recital 39).

We are also interested in the provisions in GDPR regarding the timing involved in collection, processing and notifying subjects about the collection and processing of data.

Feedback, as a design solution to provide visibility of system status, must be close in time to the events that cause change in system status to be understood as such and allow users to predict system behaviour. However, in case a data subject requires information from a controller, the response from the controller may take one month, with two months more of allowed extension.

Article 13 of GDPR makes a statement about the moment in time when information should be provided by controllers to subjects: "1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained [emphasis added], provide the data subject with all of the following information [list of information follows]".

This moment in time is hard to define. The emphasized expression can mean that the information should be provided before data is collected, as usual in informed consents, but it can be interpreted as the availability of that information at the precise time that data is collected, notifying the subject of collection and processing.

4 Experimenting Active Disclosure

This section describes the experiment we have performed to assess the impact of feedback on data subjects' perception of transparency. Our hypothesis was that a continued experience of active disclosure would change the subjects' perception regarding data collection and processing policies.

The experiment consisted in collecting subjects' opinion on transparency issues and identifying their attitude towards analysing terms of usage and privacy policies, before and after the usage of an Android application that monitored data upload activity.

Our application presented a notification when data uploaded reached a given amount. The notification was designed to be minimally intrusive as the user could receive many instances of the notification during the day.

Mobile applications were preferred to desktop applications as the data-driven target services because (1) people carry their smartphones with them, thus the instantaneous notification had the chance of being be noticed; (2) the process of installing applications is frequent, thus there is a chance that the person has been exposed to the need to evaluate service policies.

4.1 Research Question

We proposed the following research question: "does notification of data collection activity (feedback) change the subjects' attitude towards data policies?

4.2 Limits of Validity

The following facts limited the validity of the experiment.

- The experiment was performed only with mobile digital services
- The notification expresses the amount of data uploaded, not the *personal* data upload.
- The number of participants was too small to allow generalization of findings.

4.3 Description of the Experiment

The experiment was organized in two phases. In the first phase, the objective was to understand participants' perception regarding PDT. In the second phase, the participants were invited to use an application that notifies them on data collection, after which they were invited to assess the change in their perception of PDT.

First phase: survey about perception of PDT
The first survey intended to collect participants' perception about PDT. Participants were invited to participate of the study by messages widely disseminated in social networks. The survey was prepared with Google Forms, in five sections:

1. Title and explanation of the terms of use of the research, stating the objective and the rights of the participants according to Brazilian ethical procedures related to Research with Humans in the Social Sciences [8];
2. Demographics: age, monthly income and education level;
3. Technological profile: time of usage of smartphones; frequency of usage of popular applications (Google Maps, Waze, Facebook, Twitter, Instagram, WhatsApp and email);
4. Participant's perception about personal data and their applications installed on their devices, further explained;
5. Invitation to participate in the second phase (requiring the provision of the participant's e-mail address).

The questions on the perception of personal data were preceded by this explanation, in equivalent Portuguese:

> *"Currently, many companies that provide digital services collect personal data from users, stating that this action is essential to improve users' experience with their products.*
> *Personal data means data relating to a person that can identify the person, either alone or together with other data. Examples of personal data are: CPF, personal characteristics, behavior, preferences, relationships, health information.*
> *The usage terms and privacy policies of these digital services should state what data is collected, the frequency of collection, and how this data is used."*

Subsequently, participants were asked to rate their experience with PDT, answering the following questions:

- Do you remember any application on your smartphone informing you that it collects and/or shares your personal data during its use? (*Answers: Yes|No*)
- How often do you read the terms of use and privacy policies of an application? (*Answers: Never|Rarely|Frequently|Always*)

- If you answered something other than "always" in the previous question, explain why you do not read the terms of use and privacy policies. Select the alternative that best explains your attitude. (*Answers could be one of the following options or an open answer:*
  - *The policy texts are too long.*
  - *The terms of the policies are difficult to understand.*
  - *I do not know where to find the policies in the applications.*
  - *It's no use reading because the policies protect the rights of who makes the application and not mine.*
  - *It's no use reading because if I do not agree I will not be able to change anything.*
- Has some application you installed on your smartphone given you the opportunity to choose which of your personal data you authorize to collect? (*Answers: Yes|No*)
- Has some application you installed on your smartphone allowed you to select which forms of usage you authorize the app to apply to your data? (*Answers: Yes|No*)
- Please comment on the two previous questions. Do you remember which app and your answer? (*Open answer*)
- Would you stop to use an app or website if you found out that it collects and/or shares your personal data? (*Answers: I would certainly stop using| I would probably stop using| I would not stop using).*
- Please explain your choice in the previous question. (*Open answer*)

The first phase was run for one week with Brazilian participants, in June 14-21, 2018, a few days after GDPR became enforceable in Europe. We obtained 130 responses.

Second phase: installation and usage of the feedback application
Participants who expressed their interest in participating in further steps of our research provided a contact e-mail in the first phase survey form. 72 participants agreed to participate.

On June 21 2018, we sent these participants an e-mail containing the feedback application in *apk* format, the procedures for installation, operation and uninstallation. They were asked to install the app and use it for at least one day.

The application is detailed further.

Second phase: survey about changes in the perception of PDT
After 1 week of sending the application, a questionnaire was sent to all participants who consented in using the application. The intention of this questionnaire was to identify changes in user attitude towards PDT.

The questionnaire also used Google Forms in one single section, in which the following questions were presented:

- Please fill in your email so that we can relate the answers to the first part of the survey. (*Open answer*)
- How surprised you felt with the data collection feedback presented by our prototype? Consider "1" as little surprised and "5" as extremely surprised. (*Answer: 1|2|3|4|5*)
- How much has your experience with data collection feedback changed your awareness of your personal data? Consider "1" as no change and "5" as a complete change. (*Answer: 1|2|3|4|5*)

- Based on your experience with the prototype, how often will you read the terms of use and privacy policies of an application? (*Answer: Never|Rarely|Frequently|Always)*
- Based on your experience with the prototype, would you stop to use an app or website if you found out that it collects and/or shares your personal data? (*Answers: I would certainly stop using| I would probably stop using| I would not stop using).*

The last survey was run for 11 days, from June 25 to July 4,2018. As expected, many participants did not engage with the last phase. Only 23 of the 72 participants that were originally interested in participating installed the application and sent their answers.

4.4 Description of the Feedback Application

In order to provide the instantaneous feedback on data collection, we developed an Android application that met the following functional requirements:

1. The app monitors the amount of data uploaded;
2. The app notifies the user every 2Mbytes of data uploaded by issuing a continuous, 2-sec long vibratory signal;
3. Upon users' request, the app displays the total amount of data uploaded since the app activation;
4. User can turn the application on/off;

Also, the app met the following non-functional requirements:

5. Notification is minimally intrusive but non-negligible;
6. Notification is distinguishable from other applications' notifications;
7. The app does not collect or process any personal data;
8. The app runs in the Android platform (chosen because of its large market share in Brazil;
9. The app does not require root access to the user's smartphone;
10. The app installs with no need of user interaction apart from the acceptance of the installation process;
11. The app uninstalls with no traces left.

It is important to notice that the feedback app does not identify which application is responsible for data upload. While this seemed to be an interesting information to be presented to the user, the implementation of this feature would require the user granting permission in installation. We discarded this option because of the risk of mistrust.

The final version is an application that runs as a service (in background), continuously monitoring the network activity. Notification is generated whenever 2 MB of data is uploaded, by vibrating the device for 2 s and displaying a notification icon in the status bar. Also, if the user opens the notification drawer, the application displays a screen that shows the amount of uploaded data in megabytes and time since when the app started to run.

The intended usage scenario is the following: "Carmela received the app by email this morning, together with the instructions for installation and uninstallation. She

installed it easily while having breakfast. In the first hour of app operation, Carmela did not notice any difference in her smartphone, as she drove to work. In the parking lot, however, the phone vibrated for 2 s, which was unusual. She looked at the screen with strangeness, but soon recognized that the vibration was the app notification that her applications had uploaded 2Mbytes. In fact, that was exactly the displayed information she found when she clicked the app icon. During the morning, as she worked, the 2-s vibration happened again for three times. As she had not accessed any application in her smartphone in that period, she wondered which application was uploading data. During lunchtime she accessed Facebook and Twitter, as well as her email, and the app presented a more frequent notification pattern that was compatible with her activity. Good, she thought, this makes sense. In the afternoon, again she left her phone resting in her table, and now and then the vibrating notification sounded. During dinner, she talked to her husband about privacy and personal data collection, while uninstalling the app. She said, I wonder what these applications were talking about me!"

Figure 1 shows the screens that informs total uploaded data.

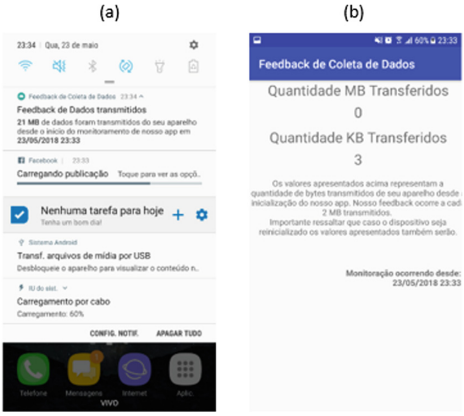

Fig. 1. Screenshots of feedback application. (a) brief notification (drawer) with totals from monitoring start time. (b) full display with information on data uploaded.

For monitoring uploaded data, we used the "getTotalTxBytes" method of the "TrafficStats" class, available from API 8 of the Android SDK [9]. This version is supported by many devices. According to the Android documentation, this method "returns the number of bytes transmitted since device boot. It counts packets across all network interfaces, increasing monotonically since device boot. Statistics are measured at the network layer, so they include both TCP and UDP usage"

The application code is available at https://drive.google.com/file/d/1gWwrtBygelfYOz3ancFsptc05hRBBzeR/view?usp=sharing.

5 Results

In this section, we present the results obtained in the three phases of the experiment.

5.1 Demographics

130 people participated of the first phase, from which 23 participated also in the second. Figure 2 describes age and Fig. 3 describes educational level of participants.

Participants age is from 17 to 68 y-o, with median of 31 y-o in phase 1. In phase 2, participants' age is from 17 to 65, with median of 28 y-o.

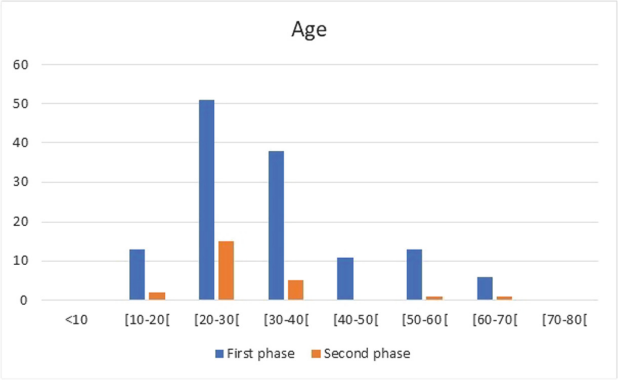

Fig. 2. Demographic profile of participants: age

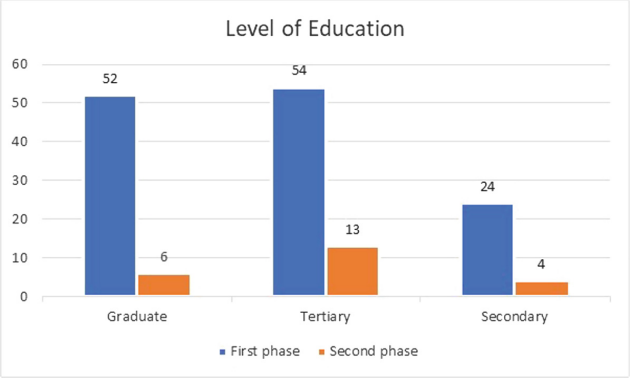

Fig. 3. Demographic profile of participants: level of education

5.2 Technological Profile

Technology profile intended to discriminate participants according to their technological expertise and frequency of usage of common mobile applications. Figure 4 shows the usage of technology.

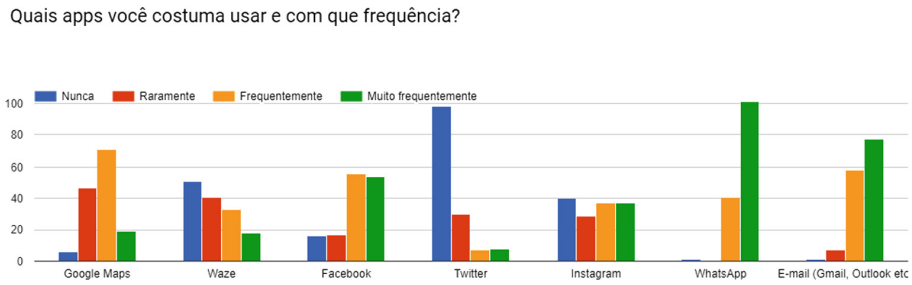

Fig. 4. Phase 1, technological profile

5.3 Perception of PDT Before Exposition to Feedback

The first phase survey showed, in general, that participants are aware of data collection but do not pay attention to terms of use and privacy policies.

74% of participants remember some application informing that it collects/shares personal data.

86% of participants declared never or rarely read an application terms of use or privacy policies. Figure 5 presents the distribution of answers.

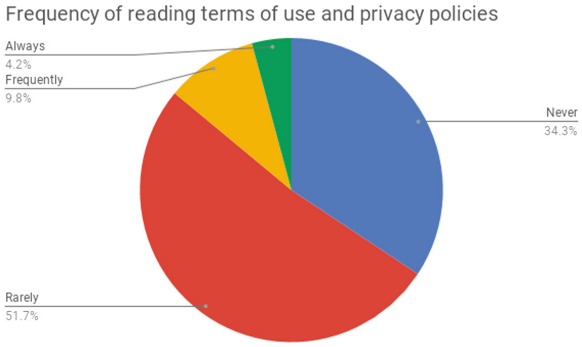

Fig. 5. First phase, frequency of reading terms of use and privacy policies

The main reason for not reading the terms is because they are too long. Table 1 shows other answers, considering that participants were requested to mark only the reason that apply in most cases.

Table 1. Reasons for not reading policies (participants marked only one)

Reasons for not reading policies	%
The policy texts are too long	47,7
The terms of the policies are difficult to understand	6,2
I do not know where to find the policies in the applications	0
It's no use reading because policies protect the rights of who makes the application and not mine	4,6
It's no use reading because if I do not agree I will not be able to change anything	27,7
Other reasons	6,1
No answer	7,7

Other reasons mentioned include carelessness, lack of time, trust in the company that uses the data, similarity between texts and herd behaviour.

Most participants were unsure whether they would cease or not to use an app or service if they found that their personal data was collected and/or shared, as shown in Fig. 6.

Those who would certainly stop using justify their decision based on the perception of privacy ("I value the right of being anonymous, especially in internet. I am not comfortable when I find out that a company is selling my personal data. I don't agree with this, but I know it's very common nowadays"), ownership of data ("Nobody has the right to use my data without my consent", "My data is my data"), perception of personal risk ("The risk of having my data explored makes me protect myself ceasing to use the application", "Certainly my data will not be used to my benefit!").

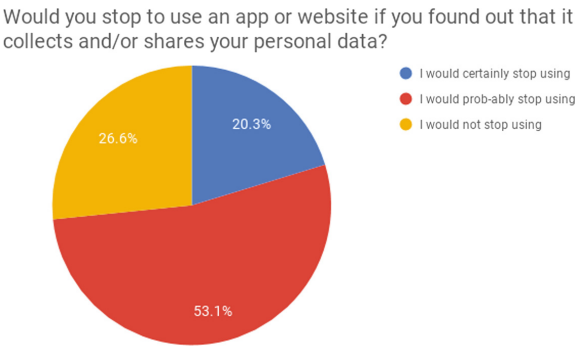

Fig. 6. Attitude towards ceasing to use an application after evidence that it collects or shares personal data

Participants that declared they would keep on using the applications justified their opinion based on service utility ("If I denied my data I would not be able to use it and I need it badly", "I choose the services based on their functionality.", "They make my life much easier"), on the feeling of helplessness because data is already public ("Our

personal data are already in the internet, there is nothing we can do about that.", "I use my smartphone for such a long time, everybody has my data", "I have nothing to hide"), the perception that the data is a fair price for free services and recommendation ("The company must make some money, so they sell my data; and doing that they send me advertisements that I may like."). Some participants say they select the data they consent in sharing ("I control myself regarding what I share in these tools").

Participants that stated they would probably stop using the application justified their answers based on several dependencies: on perceived necessity of the service, on sensitiveness and intimacy of data, on the potential of damage to the person, on companies sharing data, on the type of information collected. As for the latter, some protect specific data: they are not willing to share location, access to camera and contacts.

5.4 Change in Attitude After Exposition to Feedback

The number of participants who answered the second questionnaire is too limited to allow quantitative results (23 out of 130) however, they indicate a behaviour that can be further explored in more extensive studies.

10 out of the 23 participants of the second phase rated their surprise with the collection of data after the experience of feedback as extreme, as Fig. 7 shows.

Analysing the answers of the population that participated in both phases of this research, we observe that there is a change towards more attention to terms of usage and privacy policies of services. If we associate the answers never/rarely/frequently/always as a linear scale, Fig. 8 shows that most participants changed at least one point towards being more careful with reading these terms.

Finally, Fig. 9 shows that participants did not reject the usage of the applications when they learn that they collect and/or share users' personal data. Instead, all participants either maintained their attitude or became more tolerant to usage of personal data. This finding suggests that awareness is not a determinant factor for acceptance or rejection of a data-based service of application.

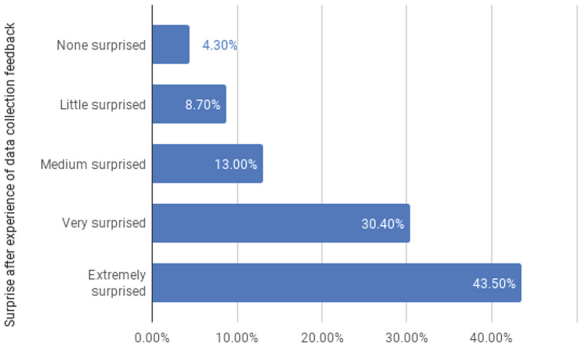

Fig. 7. Participants' feeling of surprise after experience of data collection feedback

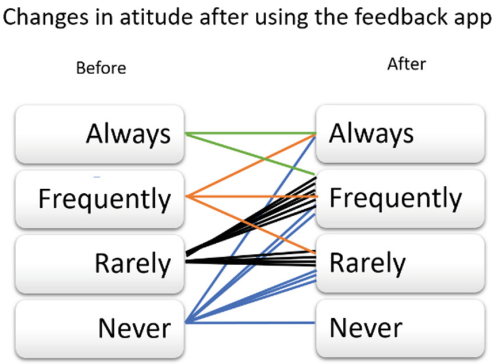

Fig. 8. Change in attitude towards reading policies, after usage of feedback application, subjects participating in both questionnaires

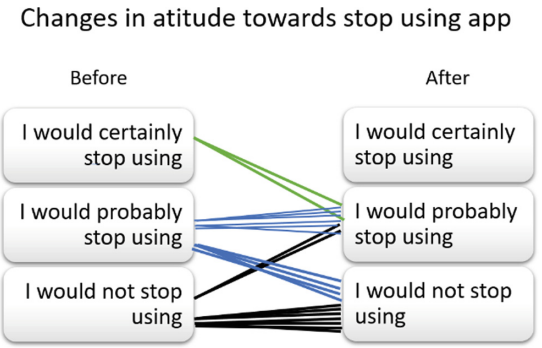

Fig. 9. Changes in attitude towards ceasing to use an application after evidence that it collects or shares personal data

6 Discussion

The analysis of participants' opinion, although not statistically significative, indicates that:

- The presentation of terms of usage and privacy policies do not stimulate users to read and understand them;
- Most participants are not interested in reading long texts prior to start using the services;
- Their attitude towards reading the policies change of they become continuously aware that their data is being collected.
- Their attitude towards ceasing to use an application that collects data does not change or tend to be more tolerant after they become aware that their data is being collected.

Because of the lack of interest in understanding the policies, we can discuss that the present form of transparency is equivalent to the passive transparency discussed by Oliver – the information may be available, but it depends on the will of the user to disclose the information. A large part of the research population is aware of data collection, but does not give due importance to the terms of use or privacy policies.

We advocate that continuous feedback is relevant to prepare users to understand the collection, but also the flow of subjects' data through processes. Continuous feedback moves the time displacement between the moment that the subject's conscience is formed and the moment that consent is given. In present situation, the moment that subjects are required to consent (prior to usage) is too distant from the moment in which awareness arises. When subjects are asked to consent in data collection, they are pressed against their own will to use the service. Reading text, whether long or short, in legalese or plain language, is not subjects' intention at that moment.

Of course, consent must be given prior to usage; it would not be fair otherwise. We argue that the instrument of revoking the consent will be used properly only if data collection and processing is actively disclosed. During usage, active feedback reminds subjects that data being uploaded comes at a price (sometimes minimally associated to subjects' consumption of their data allowance) and brings curiosity on what is being uploaded.

7 Conclusion

Although the theme of PDT is extremely important, many people do not realize that their data is being collected at all times; they do not read the terms of use and privacy policies, and thus do not really know what data-based service providers and data controllers can do with their data.

In this paper, we have reported our findings with an experiment of giving feedback of data collection on perception of transparency.

This work, despite having a simple proposal of feedback to inform the user when their data is being collected shows the users were surprised with the fact of the collection of data and that they had their perceptions changed regarding PDT, especially when it comes to reading the privacy policies of a service.

These findings suggest that visibility of the state of the system for the data collection collaborates to system legibility. Systems thus need not only to be transparent about personal data, but to promote active disclosure of data usage.

It is important to notice that in our experiment, the feedback given to our subjects was not associated to personal data upload, but any data. They were free to envisage the association between their behaviour using applications and the uploaded data. That is, the intention of the application was not to inform on the fact that personal data was being uploaded, but to create the conscience that data, whatever its nature, was being uploaded.

Because our research was carried on close to the GDPR enforcement, we believe that many subjects were not yet familiar with the discussion that came afterwards. Two participants in the first survey have asked researchers to try the application after the

research was closed. Both informed that they remembered the invitation after having contact with the PDT issue.

Data collection feedback aims to change the way subjects understand their personal data, raising more importance to this concept, educating them not to disregard the terms of use and privacy policies, understanding their rights, and even questioning whether the use of a digital service is worth, if your personal data must be given in.

We expect this work to contribute to companies, in order to motivate them to perceive the trend of subjects' behaviour change after the experience of feedback. Companies that collect, distribute or consume personal data from users can exploit feedback to increase user trust in their services and even improve their image to the market. Finally, we expect to contribute the evolution of policies, showing the importance of active disclosure on collection, distribution and consumption of their personal data, in an instant and continuous manner.

References

1. European Union: Regulation 2016/679 of the European Parliament and the Council of the European Union of 27 April 2016 on the protection of natural person
2. Mortier, R., Haddadi, H., Henderson, T., Mcauley, J.: Human-data interaction. In: Soegaard, M., Friis Dam, R. (eds.) The Encyclopedia of Human-Computer Interaction, 2nd ed. The Interaction Design Foundation
3. Oliver, R.: What is Transparency?. McGraw-Hill, New York (2004)
4. Nielsen, J.: 10 Usability Heuristics for User Interface Design, https://www.nngroup.com/articles/ten-usability-heuristics/. Accessed 14 Feb 2019
5. Johnston, J., Eloff, J., Labuschagne, L.: Security and human computer interfaces. Comput. Secur. **22**(8), 675–684 (2003)
6. Mackinlay, M.: Phases of accuracy diagnosis: (in)visibility of system status in the Fitbit. Intersect: Stanf. J. Sci. Technol. Soc. **6**(2), 1–9 (2013)
7. Harley, A.: Visibility of system status. https://www.nngroup.com/articles/visibility-system-status/?lm=match-system-real-world&pt=article. Accessed 14 Feb 2019
8. Brasil. Conselho Nacional de Saúde. Resolução 510 (2016)
9. Google Developers documentation on TrafficStats class. https://developer.android.com/reference/kotlin/android/net/TrafficStats. Accessed 14 Feb 2019