Bachelor's thesis

Information Technology

2016

Xi Chen

PRIVACY OF MOBILE APPLICATIONS

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR'S | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information Technology

2016 | 34

Xi Chen

PRIVACY OF MOBILE APPLICATIONS

With the development of smartphones, mobile applications have become an essential part of our daily life. However, the more tasks we try to perform on mobile devices, the more information about us can be collected. Thus, privacy issues of mobile applications are gaining increasing attention.

The purpose of this thesis was to analyze current privacy notices framework, to determine whether they function as expected, and to introduce a proposal which might improve the situation.

In order to analyze the effectiveness of current privacy notices framework for smart phone applications, real world applications examples were used to show how the framework was implemented , which is followed by a psychological analysis about why they did not work satisfactorily. At last through introducing Platform of Privacy Preferences Project (P3P) and analyzing the reasons for its failure, a promising proposal could be conceived.

Current privacy notices in mobile applications are well-designed, however, users continue to ignore most of them.Although there is already a systematic design space and paragon applications to follow, privacy notices do not work out effectively as they ought to. The key point is that most people care little or only partly care about their privacy, so focusing on how to make notices more understandable and usable appears to be a wrong direction from very beginning.

In conclusion, mobile applications need a standard for privacy settings and notices. More than 10 years ago there was a standard called P3P which was proposed to release users from reading complicated web sites privacy policies and automatically apply their privacy

preferences. Yet time has proved P3P was not successful but why it failed actually indicate the potential of the proposal in this thesis.

KEYWORDS:

Privacy policy Privacy notice Privacy nudge

CONTENTS

PICTURES

TABLES

LIST OF ABBREVIATIONS (OR) SYMBOLS

Abbreviation	Explanation of abbreviation (Source)
PIA	privacy impact assessment
LED	light-emitting diode
P3P	Platform of Privacy Preferences Project

1 INTRODUCTION

Technology is developing at a tremendous speed nowadays and undoubtly it will only grow even faster. For example, the smart phone, which has already made several traditional electronic devices such as watches, cameras, mp4s totally redundant, is gaining more power from upgraded hardware or applications. However, with every step the smart phone walks into our daily life, it inevitably acquires and uses our personal information, which may or may not be, in the way that we expected. One could easily steal users' money if he somehow acquires other users' bank account and password through hacking their PayPal application, which of course is not likely to happen. However the common privacy violation, which is taking place everyday, does not usually have any obvious impact on normal individuals---due to the break-through in analyzing big data some trivial information may be gathered by companies without notification, or simply be annoying---, millions of people in China receive numerous advertising phone calls and have no idea how have their numbers been compromised. Therefore, privacy issues are gaining, and should gain, increasing attention from developers of applications, while not so much among the normal users, which causes the tricky situation that emerges. When the designers of applications are dedicated to satisfying every possible privacy requirement, and ponder to write an informative privay policy notice, the users simply ignore these effort or even express impatience. This thesis is based on several research studies carried out by pioneers in the field of privacy combined with some psychological analysis, focusing on illustrating why the dilemma exists and how we should proceed with privacy in mobile applications.

2 PREVIOUS WORK ABOUT PRIVACY NOTICE DESIGN

This chapter will demonstrate how privacy policy should be implemented, compared with how it is actually implemented in real world applications.

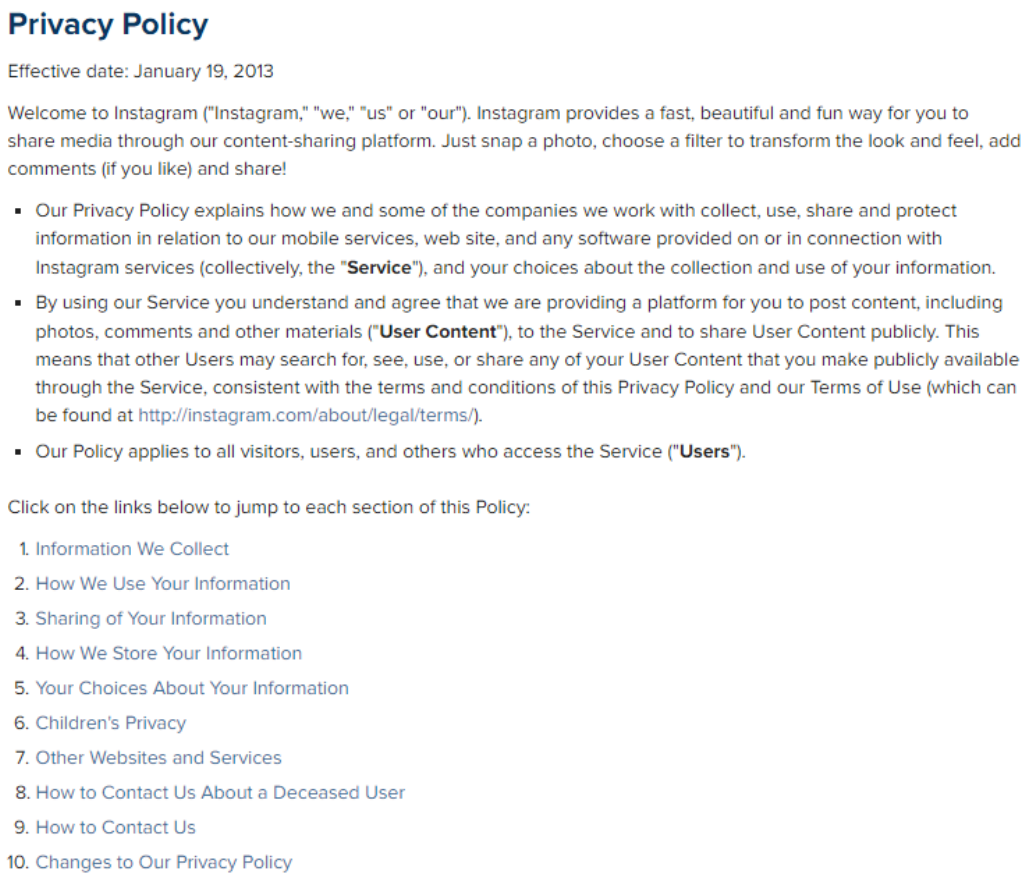
2.1 Privacy policy

Privacy policy is a legally binding document that precisely defines what and how users' personal data will be used. It also functions as a guideline of following privacy notices designing so it should be finished in the designing phase of building an application before any implementation. In order to make a flawless privacy policy, the working process of the application has to be carefully reviewed so that any data flow can be tracked, for the sake of determining whether and what privacy notices are needed. This reviewing procedure, which is called privacy impact assessment (PIA) [1], would also assess possible privacy risks according to related local laws and even produce impact on the designing of the application, ensuring that the application is completely legal and complying with regulations. Due to the rising importance of privacy, PIAs are becoming necessary or even compulsory in some countries [2]. A refined report produced by a thorough PIA significantly improves the quality of privacy policy and the application itself. Additionally it helps the designers foresee the constraints which will be encountered due to privacy so they will not have to, if being enough unlucky, rebuild the whole application because of trying to perform a single improvement or being forced to do so by law.

As their counterparts of websites, privacy policies of applications are also verbose, esoteric and extremely time-consuming to read that even IT-related personnel are not willing to read it, not to mention the general public. However right now privacy policies are still the most important source for those who want to figure out how the data is collected and processed. Just as mentioned above an ideally privacy policy has positive and decisive impact on designing an application---mostly about the privacy notices in it, the level of understanding of

a privacy policy among users also directly decides their ability to use the application efficiently and safely. More specifically, users will not be able be gain information and make an effective privacy choice during the use of an application if they do not comprehend its privacy policy from the beginning. The detailed statistics and related analysis of users' understanding of privacy policies will be included in chapter 3. At this point we could just conclude that privacy policies are expected to be not only regulatively accurate and comprehensive enough to state every detail about the privacy of the application, they should also be simple enough for a "lay person" to understand.

Here are some privacy policies of well-known applications.



Privacy Policy

Effective date: January 19, 2013

Welcome to Instagram ("Instagram," "we," "us" or "our"). Instagram provides a fast, beautiful and fun way for you to share media through our content-sharing platform. Just snap a photo, choose a filter to transform the look and feel, add comments (if you like) and share!

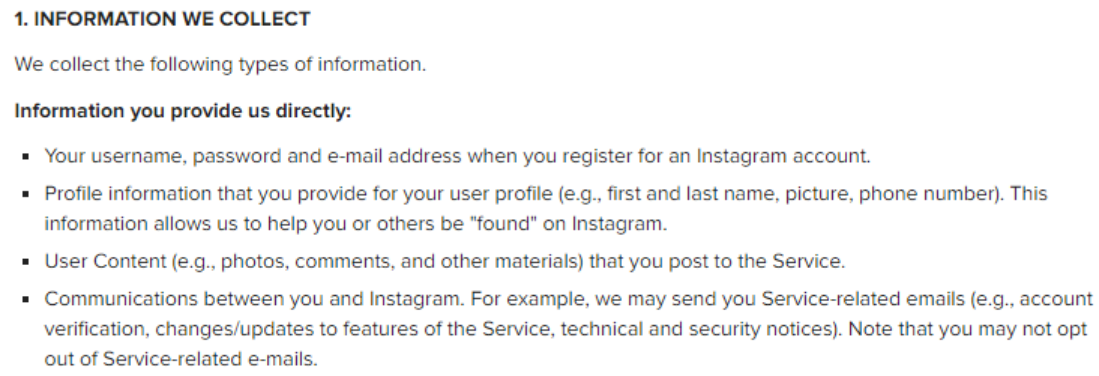
- Our Privacy Policy explains how we and some of the companies we work with collect, use, share and protect information in relation to our mobile services, web site, and any software provided on or in connection with Instagram services (collectively, the "**Service**"), and your choices about the collection and use of your information.
- By using our Service you understand and agree that we are providing a platform for you to post content, including photos, comments and other materials ("**User Content**"), to the Service and to share User Content publicly. This means that other Users may search for, see, use, or share any of your User Content that you make publicly available through the Service, consistent with the terms and conditions of this Privacy Policy and our Terms of Use (which can be found at http://instagram.com/about/legal/terms/).
- Our Policy applies to all visitors, users, and others who access the Service ("**Users**").

Click on the links below to jump to each section of this Policy:

1. Information We Collect
2. How We Use Your Information
3. Sharing of Your Information
4. How We Store Your Information
5. Your Choices About Your Information
6. Children's Privacy
7. Other Websites and Services
8. How to Contact Us About a Deceased User
9. How to Contact Us
10. Changes to Our Privacy Policy

Figure 1. Instagram privacy policy overview. [3]

Figure 1 displays a screen shot of the overview of the privacy policy of Instagram. It actually has a menu so that people can both easily have a clear general view of what it is about and simply jump to the parts they are interested in.



1. INFORMATION WE COLLECT

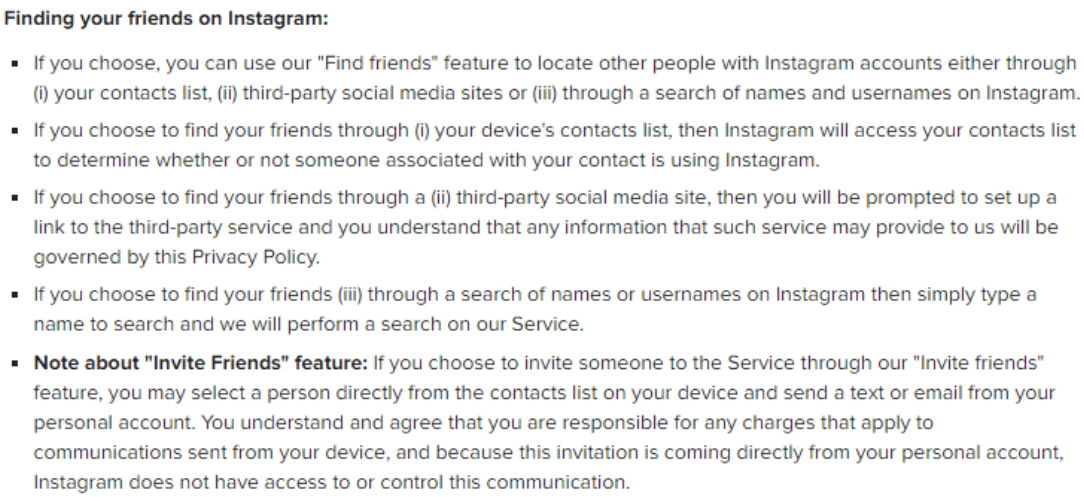
We collect the following types of information.

Information you provide us directly:

- Your username, password and e-mail address when you register for an Instagram account.
- Profile information that you provide for your user profile (e.g., first and last name, picture, phone number). This information allows us to help you or others be "found" on Instagram.
- User Content (e.g., photos, comments, and other materials) that you post to the Service.
- Communications between you and Instagram. For example, we may send you Service-related emails (e.g., account verification, changes/updates to features of the Service, technical and security notices). Note that you may not opt out of Service-related e-mails.

Figure 2. Instagram privacy policy---terms explanation. [3]

Figure 2 shows of the first part of the main body of the Instagram privacy policy. Even for those common terms that everyone knows, examples are still given.

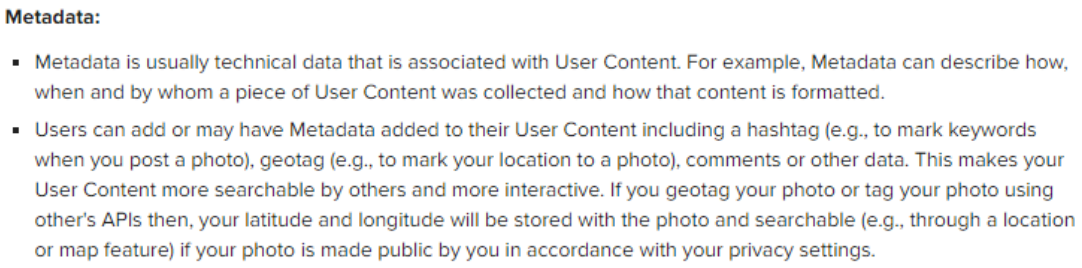


Finding your friends on Instagram:

- If you choose, you can use our "Find friends" feature to locate other people with Instagram accounts either through (i) your contacts list, (ii) third-party social media sites or (iii) through a search of names and usernames on Instagram.
- If you choose to find your friends through (i) your device's contacts list, then Instagram will access your contacts list to determine whether or not someone associated with your contact is using Instagram.
- If you choose to find your friends through a (ii) third-party social media site, then you will be prompted to set up a link to the third-party service and you understand that any information that such service may provide to us will be governed by this Privacy Policy.
- If you choose to find your friends (iii) through a search of names or usernames on Instagram then simply type a name to search and we will perform a search on our Service.
- **Note about "Invite Friends" feature:** If you choose to invite someone to the Service through our "Invite friends" feature, you may select a person directly from the contacts list on your device and send a text or email from your personal account. You understand and agree that you are responsible for any charges that apply to communications sent from your device, and because this invitation is coming directly from your personal account, Instagram does not have access to or control this communication.

Figure 3. Instagram privacy policy---user guiding content. [3]

Figure 3 illustrates the scenario that privacy policy help users to use the application more efficiently, while it does not forget to declare the users' responsibility.



Metadata:

- Metadata is usually technical data that is associated with User Content. For example, Metadata can describe how, when and by whom a piece of User Content was collected and how that content is formatted.
- Users can add or may have Metadata added to their User Content including a hashtag (e.g., to mark keywords when you post a photo), geotag (e.g., to mark your location to a photo), comments or other data. This makes your User Content more searchable by others and more interactive. If you geotag your photo or tag your photo using other's APIs then, your latitude and longitude will be stored with the photo and searchable (e.g., through a location or map feature) if your photo is made public by you in accordance with your privacy settings.

Figure 4. Instagram privacy policy---terms explanation with examples. [3]

For those quite professional terms like metadata, the policy gives a very understandable explanation with specific examples (Fig.4).

The whole document strictly adhere to the spirit of privacy policy--- that is being comprehensive and understandable.

2.2 Privacy notice

Privacy policy itself, is a kind of privacy notice to notify the users about data practices and to enable them to make informed privacy decisions. However, privacy policy is inevitably long and exhausting to read no matter how well it is composed, being ignored by most users, and due to the relatively small screen of mobile devices the document usually looks even longer than it actually is. Considering this, designers have carried out much research and contrived more feasible notification methods other than merely a document. Former existing frameworks such as *Privacy by Design* [4] mainly focus on analyzing the data practices rather than privacy notice design. For a long time there had been no standard or principle to direct how privacy notices should be designed until the publishing of *A Design Space for Effective Privacy Notices* [5]. The design space

systematically presents how to design usable privacy notices, which are briefly recited here.

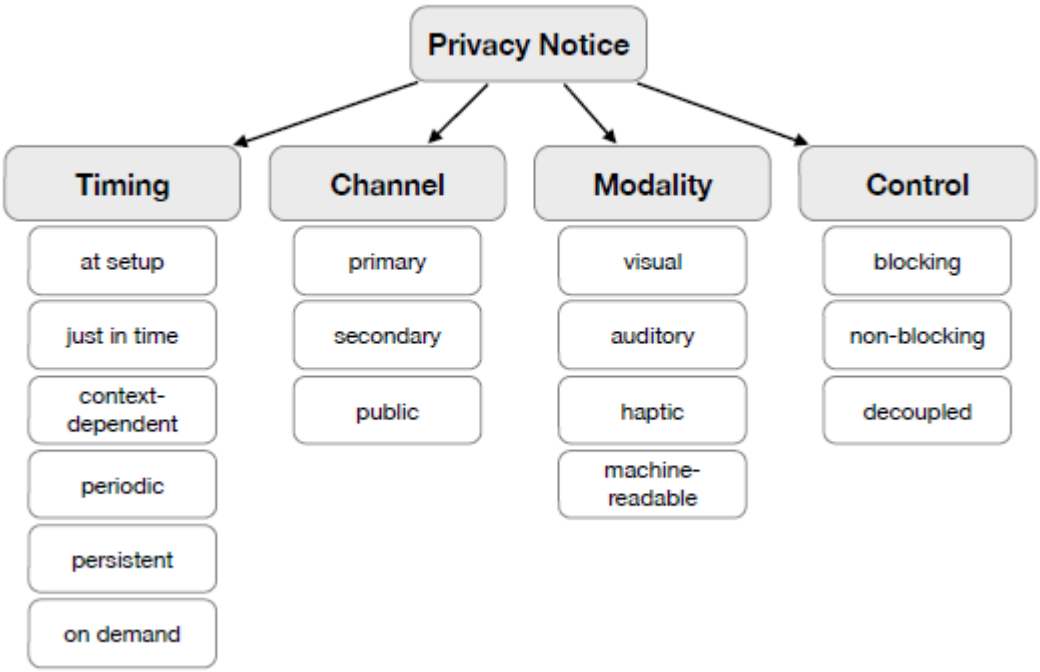


Figure 5. Privacy notice design space. [5]

2.2.1 Timing

First of all, timing has proved to be the factor which has a significant impact on the effectiveness of notices [6,7,8,9]. Notices popped up at unfavorable timing would more probably end up being ignored [10], while delay between notice and respective privacy decision also emasculates the effectiveness of the notice [11]. The general idea is that privacy notices should be adapted to the user's needs depending on timing, or more specifically, what task the user is trying to perform. As shown in Figure 5 there are six possible timing chances.

Privacy notices coming up at setup time are quite similar to the terms of use when installing a software, which most likely contain the privacy policy. One could either read it or skip it, but always be able to retrospect later. These privacy notices give

users a chance to acknowledge the data practices before starting using the application, or explanation about some unexpected situations. On the other hand, however, either because of being eager to complete and start using the application or being habituated to all kind of install-time notices, users are very likely to skip privacy notices given at setup time.

Just-in-time privacy notices show up right before data being collected, used or shared, which therefore are highly relevant to application's current task.

Context-dependent notices are referring to those notices that only show up in a specific context. For example a user might appreciate that the application asks whether to share his location when he is in a new place, regardless of his consent of sharing his location before. While this kind of notices seems pretty decent, judging the context itself usually requires access to sensitive data.

Some notices about accessing sensitive data appear with a high frequency if not disabled, which could easily lead to habituation. However, such notices are also critical and should not be disabled completely as well. To solve this dilemma, periodic notices keep users being aware of privacy-sensitive information flows while avoiding tiring the users with notice fatigue [12].

Persistent notices are usually used to indicate status, like the GPS icon in Android or IOS system. This kind of notices should not be conspicuous due to their nature, however, they are often too ambient to be noticed, too.

All privacy notices above are given to users, but users should be able to seek privacy information on their own demand. So applications should always provide methods for users to access privacy notices.

2.2.2 Channel

Different applications could use a variety of channels. In the design space channels are divided into 3 groups, primary, secondary and public.

Notices provided in primary channel mean that they are provided directly through the interface which users interact with. Thus for smart phone applications, the smart phone is the primary channel. Most notices are provided in this channel.

Secondary channels are the channels not within the devices which users interact with during using the application. For example email are used to notify users about a new reply in Instagram. Notices provided in secondary channels are usually optional and require the users' consent to receive notices with the contact information they submit during setup [13].

A public channel, as the name suggests, is the kind of channel available for everyone but merely targeted users.

2.2.3 Modality

The right choice of modality could significantly improve the effectiveness of privacy notices. For instance when performing a task with visual attention occupied, auditory notices are obviously better than visual notices. On the other hand not all users always have all modalities available [14].

Visual notices are the most diversified ones which usually carry the most amount of information, as well . In order to be effective, notices should be short and eye-catching rather than lengthy privacy policies [15]. For example , using expectation scores to concey useful privacy information [16]. Summarizing methods, such as privacy tables or privacy nutrition labels have been proposed. Another idea is that notices could be personalized to specific users, like translating notices into users' mother language. Besides text, images, icons and LEDs are also visual notices which might convey information faster but more abstractly. Users might not understand nor notice them without being educated respectively [17].

Auditory notices can be sounds or spoken words, such as "your call might be recorded". In smart phone applications, auditory notices are mostly sounds, which could draw attention more easily than visual notices. More importantly, they could

be used to notify secondary users regardless of the primary users' subjective will. For example, the shutter sound of digital cameras on smart phones are mandatory in some Asian countries to make nearby people aware that a picture is being taken. Still, in the same way as images, icons or LEDs, users have to know the meaning of the sounds to learn the notices.

Haptic notices carry even less information than audio, but haptics is still considered to be a potential modality to transmit privacy signals. Others, like smell or taste, have not been used in smart phones yet.

Machine-readable notices are in a format that was encoded from human-readable notices and could be used in communication between devices. This means that the same notice, such as a privacy policy, could be presented differently on different devices or to different user groups. However, despite their flexibility, there is risk of misinterpretation or mispresentation. A standard format would solve this problem, like P3P, which will be presented in Chapter 4.

2.2.4 Control

Privacy notices should not only give information. This information, in many cases, is provided to prompt users' effective decision making. The two classic choice models are opt-in, which means users must agree on the data practices to continue, and opt-out, which means users could disable designated data practices. Well-designed privacy options should separate function modules according to respective data practices so when disabling a certain data practice the application will not lose all functions [18]. However, elaborate privacy notices do not always equal to good privacy notices in this scenario, that users might feel overconfident then overshare [19] or be unwilling to manage the complicated settings [20]. Controls integrated into notices can be blocking or non-blocking, while decoupled ones (controls which are given separately from the notices) could be used on users' demand.

Blocking notices typically ask for consent of the opt-in type so that before using a function, users have to authorize involved data practices, which is just similar to accepting the terms of use before installing a software. A problem is that users may become habituated to this kind of clickthrough agreements. One solution is to discard the simple yes or no button and make it more complicated so it will increase engagement. However, a complicated or time-consuming blocking notice might become annoying for users who seek a swift use experience.

Non-blocking notices with control usually apply previous settings to current ones if users do not do any specific adjustments, so they will not block anything.

Some controls are not in the application they affect, but in other special applications, such as privacy managers or privacy dashboards, which enable the users to change their settings whenever they want [21,22]. In our opinion, this is the best control type that could save tons of time for users.

3 REAL WORLD EXAMPLES AND ANALYSIS

A privacy policy is designed to protect the privacy of the clients who will use the applications. However, it often happens that end users ignore the privacy policy or do not have a chance to view the detailed privacy policy. So why does this phenomenon happen? There are several factors worth considering.

3.1 Examples of real world privacy policies, settings, and nudges

The privacy policy is not often in conspicuous places for the users to see. For example, Figure 6 clearly shows the process of how the users access an application.

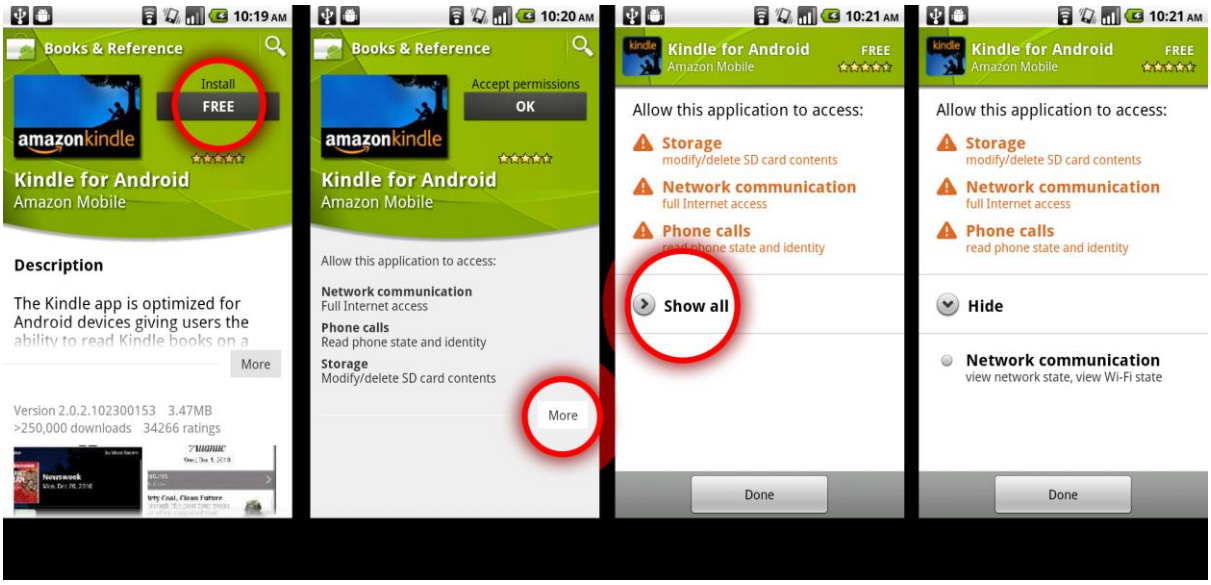


Figure 6. The visibility of privacy policy. [23]

The figure above shows the workflow for the users to install an application and to view application permissions. From the left, the first screen shows the Amazon Kindle application as displayed in the Android application store. If a user presses the "free" button, which is circled in red, the user will be led to the second screen. Screen 3 and 4 will only be shown when the user presses the "more" button in the second screen. However, since the "ok" button is at the

same place with the "free" button, if the user double clicks the button, the installation will automatically begin without showing more details of the privacy policy. In such cases, users seldom have the chances to see what the privacy policy contains. Furthermore, as the "more" button does not contain any information itself, few users will notice and be curious about what it means and what will happen when it is clicked. The urgent need to use the application will also result in a consequence of a quick installation without looking at the information other than the "ok" button.

The visibility of the private options also matters. Figure 7 shows the common settings inside a smart phone.

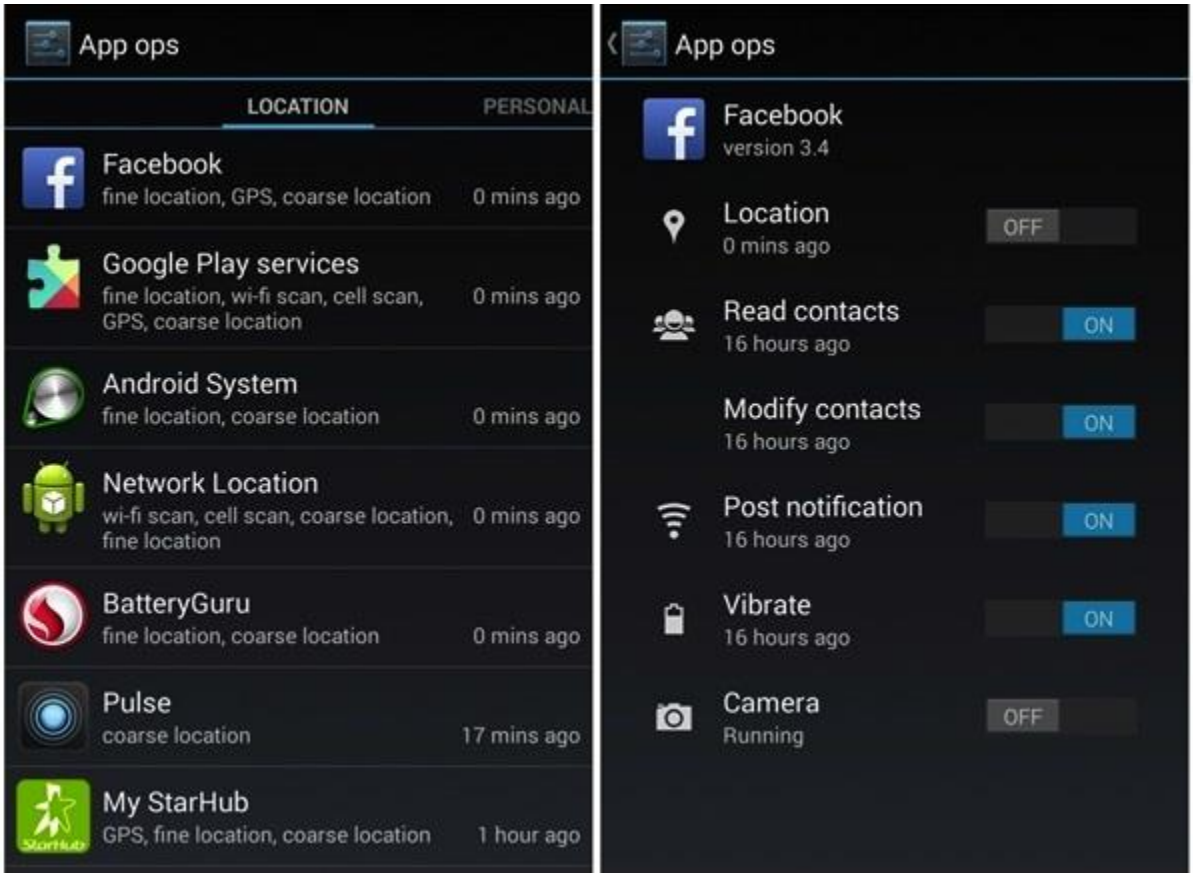


Figure 7. Common privacy settings [24]

The figure above shows when the users start to set the private options. It can be seen that all applications in the phone will be listed. When the user clicks onto one of the applications, more detailed options will be listed including

privacy options, such as the allowance to get the location of the user. Not many users access settings very often, which mainly happens when the settings violate the habit of the user of using the phone. Furthermore, there are some users who basically do not know how to configure their phones, such as senior citizens. Thus, which application has the access to private information, how applications access the information and what specific information is being used are unknown to users who do not try to understand. The truth is, most people are ignorant of the settings.

Sometimes there will be some nudge content to the users to inform them that private information is being used, as for example, in Figure 8.

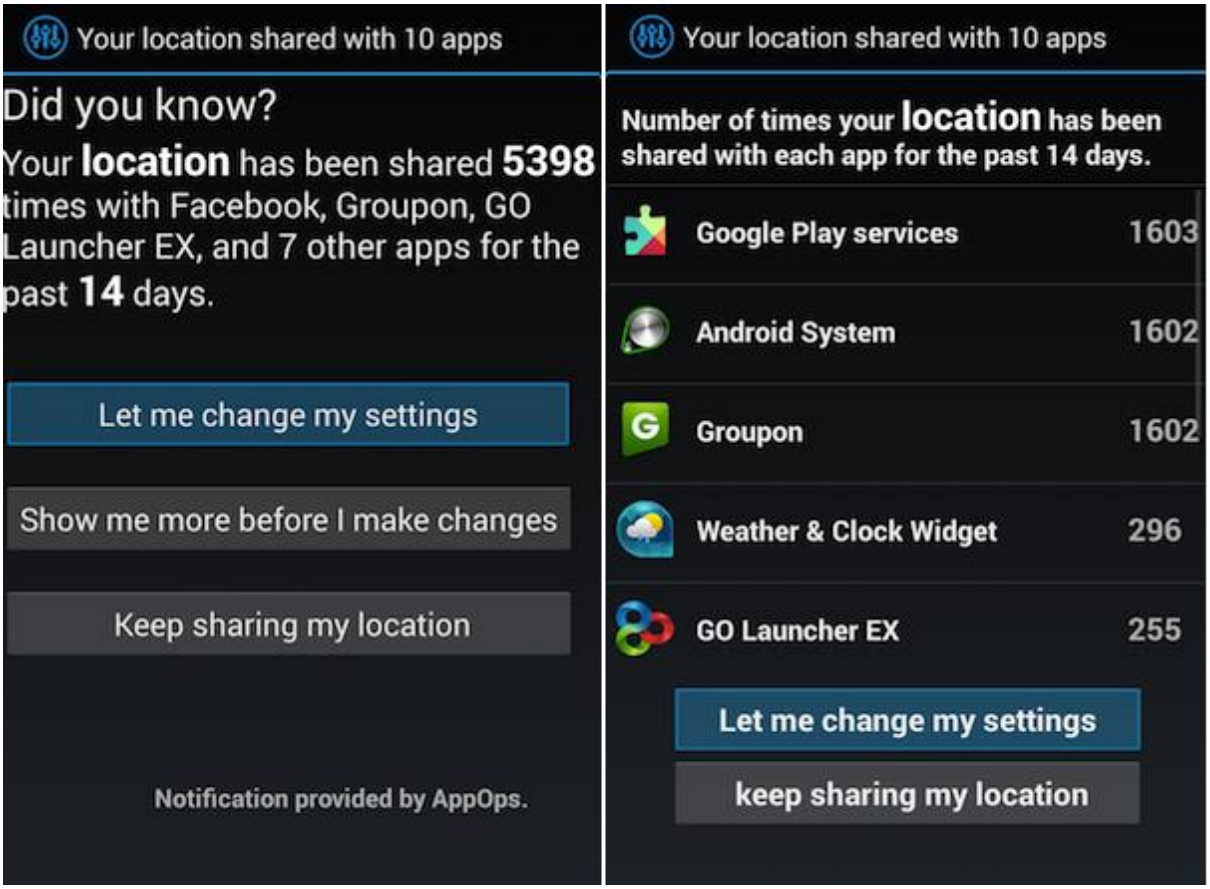


Figure 8. Nudge content example. [24]

The figure above shows that the location of the user is being used and how many applications are using the location. It allows users to change the settings if the users deem it unnecessary to share their location any longer. If the users

are indifferent to the settings and want to close the nudge window, they simply press the "keep sharing my location" button. However, how and when such nudge windows pop up needs further design because it will be annoying to suddenly see this window while playing a game or watching a video. It will also be redundant to see such windows too frequently. Thus, how to keep the user experience of high standard while nudging privacy information becomes a concern for the designers and developers of the applications.

3.2 Reasons why the effectiveness of privacy policies, settings and nudges do not meet the expectations

There are mainly three reasons why privacy policies, settings and nudges do not function as well as expected.

3.2.1 The risk of private information leakage

The privacy policy of a mobile application is originally designed to protect the private information of the end users. Thus, considering the risk of information leakage the users might ignore the privacy policy and options. Nowadays, application developers are in heated competition with each other and few dare risk violating privacy policies to expose the private information of the users for financial reward. Obviously, users whose private information is precious will definitely pay more attention to protecting their information from leakage. Violating the contract often results in severe penalty such as imprisonment and fining according to the damage it incurs. Therefore, common users are not in fear of private information leak because of the lack of value of their private information and the protection of related laws and regulations.

Furthermore, the commonly seen information utilization of applications is often of information which does not play a key roles such as current locations, which is effective temporarily, or invaluable accounts for web portals, which can be easily found back. Therefore, users do not care whether or not their information

faces disclosure. The risk of property lose or personal damage through private information leakage on a smart phone is comparatively low.

3.2.2 Opportunity cost to learn privacy policy

Generally, users will measure the cost and benefit and the efficiency between them when facing a specific task. Users will also evaluate the benefit of learning a privacy policy. If they regard it of great necessity to know every detail of it, no matter where it hides, it will be dug out and studied. Contrarily, users will ignore it if they deem it useless to know what it is talking about and how it relates to personal interests.

It is universally known that few users will look deep in what privacy policy contains. Nor does the author. From the analysis above, it can be concluded that ignoring the text in privacy policy will result in little risk. On the other hand, knowing the detail of privacy policy only helps to eliminate the risk. Thus, the cost will be the time to read and learn about the privacy policy, which is often very long and detailed. The benefit will be controlling the insignificant risk of information leakage. It is not difficult to evaluate the relationship between cost and benefit. AS the pace of life becomes quicker and quicker, users value convenience more than ever. Even tutorials are omitted in modern applications. Taking time to read privacy policies obviously violates the basic concept of convenience.

3.2.3 Popularizing rate of privacy policy

The reality, due to survey and the analysis above, is that few users know exactly what the privacy policy of a mobile application includes, including whether the application collects personal information and under what circumstances the information will be collected.

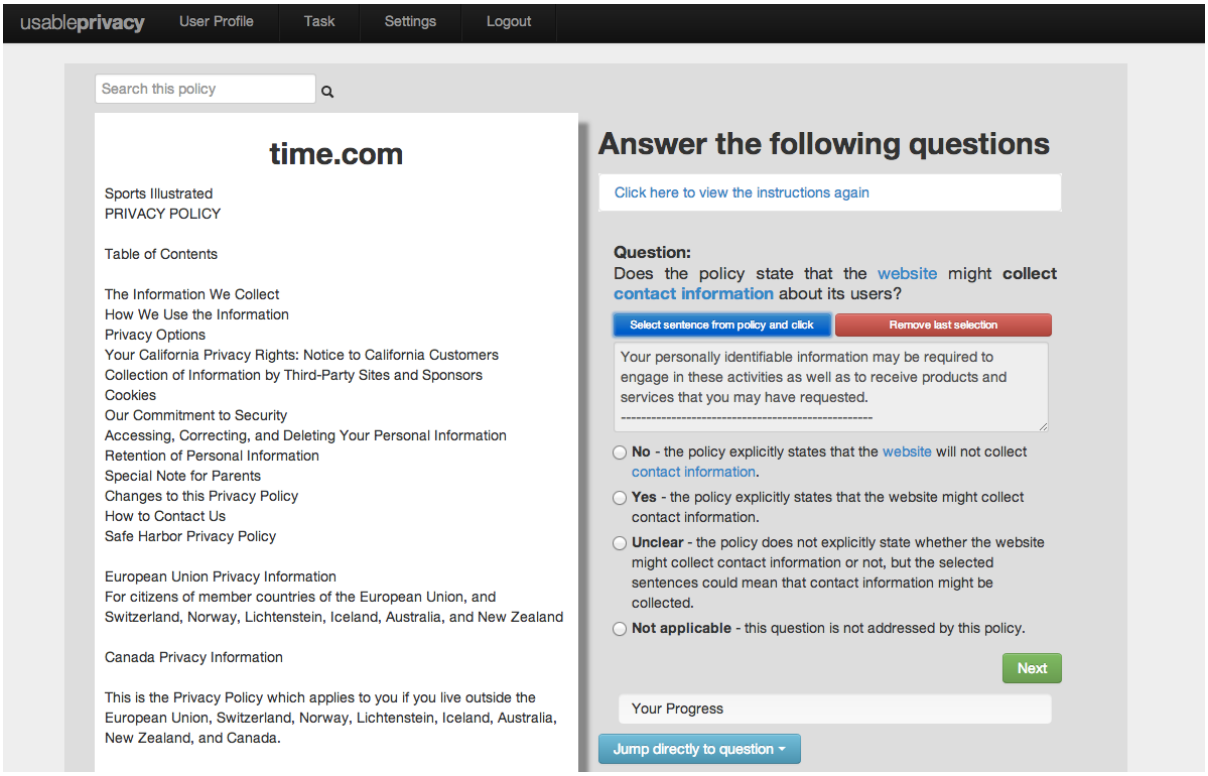


Figure 9. Online survey about understanding of privacy policies. [25]

Figure 9 shows an online survey that examines how users understand privacy policies. There are basically four options which differ the extent that the privacy policy collects personal contact information. The survey results were classified by different groups of users including experts to common users. The result showed that few users, the experts, showed a certain level of accuracy to the question, knowing whether the application collects personal information, with far more lay people being unclear about the policy or handing in a wrong answer.

4 POSSIBLE SOLUTION SIMILAR TO P3P

More than 10 years ago there appeared a standard which was designed to end the chaos of distrust between users and electronic commerce companies, called Platform for Privacy Preferences Project (P3P). The solution proposed in this thesis is actually inspired from P3P, although P3P itself did not work out as expected.

4.1 What is P3P and how it works

P3P functioned as a specified machine-readable language for privacy policies. The way it worked was that websites would post their privacy policies in P3P format for web browsers to download them automatically to compare with each user's privacy settings. In the event of finding a privacy policy which did not match the user's settings, actions such as alerting the user or blocking cookies would be taken automatically by the browser. P3P was offering a rich vocabulary that websites could describe their privacy practices with, which is quite different from the proposals for Do Not Track being discussed by the W3C [26]. Thus the machine-readable code would be able to be parsed to display a privacy "nutrition label" [27] or icons which could be regarded as a summary of a site's privacy practices.

As an extension protocol to the HTTP protocol, P3P relies on HTTP to function. P3P user agents send standard HTTP requests to get a P3P policy reference file from the web site being visited by the user, which contains the location of the P3P policy file. There might be one or more P3P policy for one web site, depending on whether different policies are applied to different parts of the web site. Shown in table 1 is an example P3P policy reference file:

Table 1. P3P policy reference file example.

```
<META xmlns="http://www.w3.org/2000/12/P3Pv1">
  <POLICY-REFERENCES>
    <EXPIRY max-age="864000"/> <!-- 10 days -->
    <POLICY-REF about="#policy1">
      <INCLUDE>/*</INCLUDE>
      <COOKIE-INCLUDE>* .example.com *</COOKIE-INCLUDE>
    </POLICY-REF>
  </POLICY-REFERENCES>
  <POLICIES>
  <POLICY discuri = "http://www.example.com/privacy/policy.html"
     name="policy1">

    <EXPIRY max-age="864000"/> <!-- 10 days -->
    <ENTITY>
      <DATA-GROUP>
        <DATA ref="business.name">Example Corp.</DATA>
        <!-- it's a good idea to include an email address or
             other contact information here as well -->
      </DATA-GROUP>
    </ENTITY>
    <ACCESS><nonident/></ACCESS> <!-- no identified data is
collected -->
    <!-- if the site has a dispute resolution procedure that it
follows,
         a DISPUTES-GROUP should be included here -->
    <STATEMENT>
      <PURPOSE><current/><admin/><develop/></PURPOSE>
      <RECIPIENT><ours/></RECIPIENT>
      <RETENTION><indefinitely/><RETENTION>
      <DATA-GROUP>
        <DATA ref="#dynamic.clickstream"/>
        <DATA ref="#dynamic.http"/>
      </DATA-GROUP>
    </STATEMENT>
  </POLICY>
  </POLICIES>
</META>
```

After fetching the appropriate file, the user agent parses it to compare with the user's privacy preference, and takes actions if necessary (Fig.10).

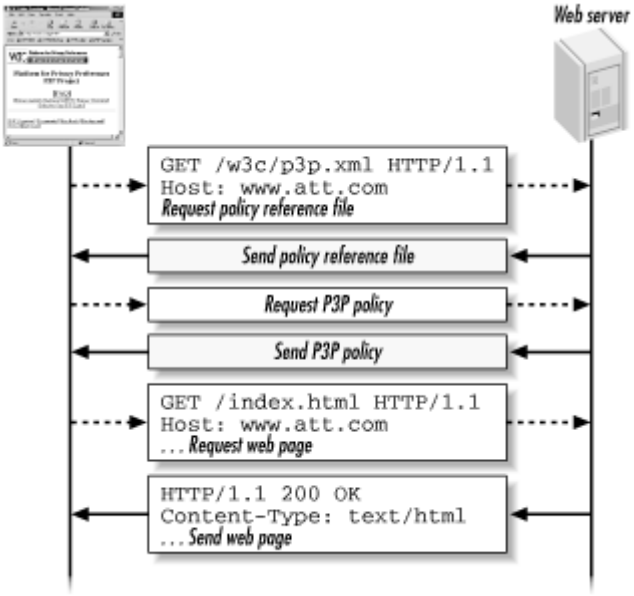


Figure 10. The basic protocol for fetching a P3P policy. [28]

Here is an example of how plain text privacy policy in English looks like. The plain text is:

Table 2. Plain text privacy policy example

Steve's Store strives to protect your privacy. When you come to our site to browse our catalog, we will not ask you to tell us who you are, and we will use data about your visit only to help us improve and secure our site. When you browse our site, we collect basic information about your computer and connection. We purge this information on a weekly basis. We also collect aggregate information on what pages consumers visit on our site. Steve's Store is a licensee of the PrivacySealExample Program. The PrivacySealExample Program ensures your privacy by holding web site licensees to high privacy standards and confirming with independent auditors that these information practices are being followed. Questions regarding this statement should be directed to: Steve's Store, 123 Steve Street, Bethesda, MD 20814 USA, Email: steve@stevesstore.com, Telephone (301) 392-6753. If you are not satisfied with our response to your inquiry, you may contact PrivacySealExample at http://www.privacyseal.example.org. Steve's Store will correct all errors or wrongful actions arising in connection with the privacy policy.

After encoded with P3P syntax, the policy looks as follows (Table 3) :

Table 3. Privacy policy encoded with P3P syntax

```
<POLICIES xmlns="http://www.w3.org/2000/12/P3Pv1">
<POLICY discuri="http://www.stevesstore.com/privacy.html"
 name="policy1">
 <ENTITY>
  <DATA-GROUP>
   <DATA ref="#business.name">Steve's Store</DATA>
   <DATA ref="#business.contact-info.postal.street">
         123 Steve Street</DATA>
   <DATA ref="#business.contact-info.postal.city">Bethesda</DATA>
   <DATA ref="#business.contact-info.postal.stateprov">MD</DATA>
   <DATA ref="#business.contact-info.postal.postalcode">20814</DATA>
   <DATA ref="#business.contact-info.postal.country">USA</DATA>
   <DATA ref="#business.contact-info.online.email">
         steve@stevesstore.com</DATA>
   <DATA ref="#business.contact-
info.telecom.telephone.intcode">1</DATA>
   <DATA ref="#business.contact-info.telecom.telephone.loccode">301</DATA>
   <DATA ref="#business.contact-info.telecom.telephone.number">
         3926753</DATA>
  </DATA-GROUP>
 </ENTITY>
 <ACCESS><nonident/></ACCESS>
 <DISPUTES-GROUP>
  <DISPUTES resolution-type="independent"
    service="http://www.PrivacySeal.example.org"
    short-description="PrivacySeal.example.org">
   <IMG src=http://www.PrivacySeal.example.org/Logo.gif
        alt="PrivacySealExample logo"/>
   <REMEDIES><correct/></REMEDIES>
  </DISPUTES>
 </DISPUTES-GROUP>
 <STATEMENT>
  <PURPOSE><admin/><develop/></PURPOSE>
  <RECIPIENT><ours/></RECIPIENT>
  <RETENTION><stated-purpose/></RETENTION>
  <DATA-GROUP>
   <DATA ref="#dynamic.clickstream"/>
   <DATA ref="#dynamic.http"/>
  </DATA-GROUP>
 </STATEMENT>
</POLICY>
</POLICIES>
```

Besides the normal format, there is a short format of policy specified for cookies, called compact policy. Cookies are the most common data which web sites track so with compact policies cookie processing could proceed simultaneously with polich evaluation. Table 4 provides an example of a server's response containing compact policy:

Table 4. Compact policy example

```
HTTP/1.1 200 OK
P3P: policyref="http://cookie.example.com/w3c/p3p.xml",
     CP="NON DSP ADM DEV PSD CUSo OUR IND STP PRE NAV UNI"
Content-Type: text/html
Content-Length: 8934
Server: CC-Galaxy/1.3.19
```

Even though P3P could be directly implemented in web browser, the implementation could take place in various tools like applications or softwares. Thus, the general term for this kind of tools is "user agent". For an example, the Privacy Bird [29] developed by AT&T Corp. Privacy Bird functions as a translator which reads the machine-readable P3P format privacy policies and display them in an language understandable for ordinary people.

4.2 Why P3P did not suceed

Unfortunately P3P , according to one of it's creator Lorrie Cranor, is all but dead and practically useless to end users. Many organizations or individuals working in related fields have been skeptical or opposing to it since its publication. One of the largest well-known critic of P3P, the Electronic Privacy Information Centre (EPIC) even published an assessment [30] which claimed that P3P as "pretty poor privacy" . First of all, P3P is machine-readable but not human-readable, even though there are P3P softwares, majority of average users actually do not know how to install or use them. Being intended to bring convenience to users, however, P3P failed to fulfil its original goal. In general, there are two main reasons for its failure, firstly lack of enforceable rules from governments and

secondly lack of incentive for companies. No one really wants to or has to adopt to it. Some industry representatives do not even hide their hatred against it, for instance Michael Kaply from IBM once said [31] :

Ah the memories.

We (IBM) wrote the original P3P implementation and then Netscape proceeded to write their own. So both our companies wasted immense amounts of time that everyone thought was a crappy proposal to begin with.

Remove it.

On the other hand, P3P is not accepted by governments as well. The European Union refused to take P3P as part of their privacy protection framework, as European Commision argued that [32] :

A technical platform for privacy protection will not in itself be sufficient to protect privacy on the web. It must be applied within the context of a framework of enforceable data protection rules, which provide a minimum and non-negotiable level of privacy protection for all individuals. Use of P3P in the absence of such a framework risks shifting the onus primarily onto the individual user to protect himself, a development which would undermine the internationally established principle that it is the "data controller" who is responsible for complying with data protection principles.

There is a risk that P3P, once implemented in the next generation of browsing software, could mislead EU-based operators into believing that they can be discharged of certain of their legal obligations (e.g. granting individual users a right of access to their data) if the individual user consents to this as part of the online negotiation. In fact those businesses, organizations and individuals established within the EU and providing services over the Internet will in any case be required to follow the rules established in the data protection directive 95/46/EC (as implemented in national law) as regards any personal data that they collect and process. P3P might thus cause confusion not only among operators as to their obligations, but also among Internet users as to the nature of their data protection rights.

These shortcomings of P3P, however, will not exist in the solution which is proposed here.

4.3 Global Privacy Configuration

Global Privacy Configuration, as the name suggests, is a configuration of user's privacy preference which affects every application on one device, or even applications on multiple devices controlled by the same account. This configuration's primary task is to avoid repeat settings. For example, if a user does not want to share his contacts, he most likely will not want to share them in any application, then in this case he could set "no share contacts" in the Global Privacy Configuration. If he changes his mind afterwards he would also only need to change the setting once but not once for each application. In addition, if a user wants to allow one or more certain applications to access his contacts, there should be a list of applications which might ask for the access in the Global Privacy Configuration so he could do the detailed adjustment easily. The Global Privacy Configuration should contain all the possible common privacy options for sensitive data practices with each data practice followed by a list of installed applications which might perform that data practice, and the user would able to give same settings for every applications in a list or different settings respectively. The idea is that, the Global Privacy Configuration should be easy enough for "lazy" users to set their preference once for all in most cases while still providing the possibility for performing most complicated custom configurations.

According to the analysis in chapter 3, people value convenience more than ever. That is why this Global Privacy Configuration would be appreciated. People would be quite willing to read those policies carefully and consider the options thoroughly if they know they could discard them once for all. On the other hand, gathering privacy options and categorizing them undoubtly increase the

understanding of the options and therefore the efficiency of using them. If the options are simply meaningless for users, they could discard them as well.

Compared to P3P, this Global Privacy Configuration does not even need enforcement from governments and since it is beneficial for users, it would surely bring benefit to companies. It could be regarded as a tool at the beginning but after users realizing its superiority and with more applications' supporting, it would become a standard which naturally standardize the privacy related application design and isolate those applications which do not comply with it, since users would become habituated to use Global Privacy Configuration rather than configure settings in individual applications.

5 CONCLUSION

Much research has been carried out to address the increasingly significant privacy issue, however, none of them discovered that convenience is the major part of users' concern. Most people do not really care about their so called "sensitive data" being exposed but only want convenience in their using experience. In the same way there is no point in trying to write delicate privacy policies since no one would read them. At any time, users' will should be considered as first priority, so the Global Privacy Configuration would be a solution to improve the effectiveness of privacy notices and settings. Since it not only save users from repeatingly configure similar privacy settings, but also provides generalized patterns in designing applications, which is actually convenience for designers.

REFERENCES

[1] D. Wright, K. Wadhwa, P. D. Hert, D. Kloza, and D. G. Justice. A Privacy Impact Assessment Framework for data protection and privacy rights. Deliverable September, PIAF project, 2011.

[2] D. Wright. Should privacy impact assessments be mandatory? Communications of the ACM, 54(8):121–131, Aug. 2011.

[3] Instagram,2013. Privacy Policy. [online] Available at: https://www.instagram.com/about/legal/privacy/[Accessed 25 May 2016]

[4] G. Danezis, J. Domingo-Ferrer, M. Hansen, J.-H. Hoepman, D. Le M´etayer, R. Tirtea, and S. Schiffner. Privacy and Data Protection by Design – from policy to engineering. report, ENISA, Dec. 2014.

[5] F. Schaub, R. Balebako, A. L. Durity, L. F. Cranor. A Design Space for Effective Privacy Notices Symposium on Usable Privacy and Security (SOUPS) 2015, July 22–24, 2015, Ottawa, Canada.

[6] R. Balebako. Mitigating the Risks of Smartphone Data Sharing: Identifying Opportunities and Evaluating Notice. PhD thesis, Engineering and Public Policy, Carnegie Mellon University, 2014.

[7] S. Egelman, J. Tsai, L. F. Cranor, and A. Acquisti. Timing is everything?: the effects of timing and placement of online privacy indicators. In Proc. CHI ’ 09. ACM, 2009.

[8] N. S. Good, J. Grossklags, D. K. Mulligan, and J. A. Konstan. Noticing notice: a large-scale experiment on the timing of software license agreements. In Proc. CHI ’07. ACM, 2007.

[9] S. Patil, R. Schlegel, A. Kapadia, and A. J. Lee. Reflection or action?: How feedback and control affect location sharing decisions. In Proc. CHI ’14. ACM, 2014.

[10] M. S. Wogalter, V. C. Conzola, and T. L. Smith-Jackson. Research-based guidelines for warning design and evaluation. Applied Ergonomics, 33(3):219–230, 2002.

[11] I. Adjerid, A. Acquisti, L. Brandimarte, and G. Loewenstein. Sleights of privacy: Framing, disclosures, and the limits of transparency. In Proc. SOUPS ’13, page 9. ACM, 2013.

[12] R. B¨ohme and J. Grossklags. The security cost of cheap user interaction. In Proc. Workshop on New Security Paradigms. ACM, 2011.

[13] Federal Trade Commission. Internet of things: Privacy & security in a connected world. FTC staff report, Jan. 2015.

[14] W3C,2010. Web accessibility and usability working together. [online] Available at: http://www.w3.org/WAI/intro/usable [Accessed 25 May 2016]

[15] A. M. McDonald and L. F. Cranor. The Cost of Reading Privacy Policies. I/S: A Journal of Law and Policy for the Information Society, 4(3):540–565,2008

[16] C. Gates, N. Li, H. Peng, B. Sarma, Y. Qi, R. Potharaju, C. Nita-Rotaru, and I. Molloy. Generating summary risk scores for mobile applications. IEEE Trans. Dependable and Secure Computing, 11(3):238–251, May 2014.

[17] M. S. Wogalter, V. C. Conzola, and T. L. Smith-Jackson. Research-based guidelines for warning design and evaluation. Applied Ergonomics, 33(3):219–230, 2002.

[18] M. Langheinrich. Privacy by design – principles of privacy-aware ubiquitous systems. In Proc. UbiComp’ 01. Springer, 2001.

[19] L. Brandimarte, A. Acquisti, and G. Loewenstein. Misplaced confidences privacy and the control paradox. Social Psychological and Personality Science, 4(3):340–347, 2013.

[20] M. J. Keith, C. Maynes, P. B. Lowry, and J. Babb. Privacy fatigue: The effect of privacy control complexity on consumer electronic information disclosure. In Proc. ICIS ’14. SSRN, 2014.

[21] Federal Trade Commission. Mobile privacy disclosures: Building trust through transparency. FTC staff report, Feb. 2013.

[22] Federal Trade Commission. Internet of things: Privacy & security in a connected world. FTC staff report, Jan. 2015.

[23] H. Almuhimedi, F. Schaub, N. Sadeh, I. Adjerid, A. Acquisti, J. Gluck, ... & Y. Agarwal(2015, April). Your location has been shared 5,398 times!: A field study on mobile app privacy nudging. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 787-796). ACM.

[24] P. G. Kelley, S. Consolvo, L. F. Cranor, J. Jung, N. Sadeh, & D. Wetherall (2012). A conundrum of permissions: installing applications on an android smartphone. In *Financial Cryptography and Data Security* (pp. 68-79). Springer Berlin Heidelberg.

[25] J. R. Reidenberg, T. Breaux, L. F. Cranor, B. French, A. Grannis, J. T. Graves, ... & R. Ramanath(2015). Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding. *Berkeley Tech. LJ*, *30*, 39.

[26] W3C,2013. Tracking Protection. [online] Available at: https://www.w3.org/2011/tracking-protection/ [Accessed 25 May 2016]

[27] CyLab Usable Privacy and Security Laboratory,2010. Privacy Nutrition Labels. [online] Available at: http://cups.cs.cmu.edu/privacyLabel/ [Accessed 25 May 2016]

[28] Web Security, Privacy & Commerce By Simson Garfinkel, Gene Spafford

[29] CyLab Usable Privacy and Security Laboratory ,2006. Privacy Bird. [online] Available at :http://www.privacybird.org/ [Accessed 25 May 2016]

[30] "Pretty Poor Privacy: An Assessment of P3P and Internet Privacy". Electronic Privacy Information Center. June 2000.

[31] M. Kaply ,2004.Comment about P3P in forum. [online] Available at: https://bugzilla.mozilla.org/show_bug.cgi?id=225287#c12 [Accessed 25 May 2016]

[32] European Commission. (1998, January). Platform for Privacy Preferences and the Open Profiling Standard. Draft opinion of the Working Party on the Protection of Individuals with regard to the processing of Personal Data. [online] Available at: http://www.epic.org/privacy/internet/ec-p3p.html [Accessed 31 May 2016] .