Negotiation as an Interaction Mechanism for Deciding App Permissions

Tim Baarslag
University of Southampton
Southampton, SO17 1BJ
T.Baarslag@soton.ac.uk

Helia Marreiros
University of Southampton
Southampton, SO17 1BJ
H.Marreiros@soton.ac.uk

Alper T. Alan
University of Southampton
Southampton, SO17 1BJ
ata1g11@ecs.soton.ac.uk

Enrico H. Gerding
University of Southampton
Southampton, SO17 1BJ
eg@ecs.soton.ac.uk

Richard C. Gomer
University of Southampton
Southampton, SO17 1BJ
r.gomer@soton.ac.uk

m.c. schraefel
University of Southampton
Southampton, SO17 1BJ
mc@ecs.soton.ac.uk

Ilaria Liccardi
MIT CSAIL
Cambridge, MA 02139
ilaria@csail.mit.edu

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the Owner/Author. Copyright is held by the owner/author(s).
CHI'16 Extended Abstracts, May 7–12, 2016, San Jose, CA, USA.
ACM 978-1-4503-4082-3/16/05.
http://dx.doi.org/10.1145/2851581.2892340

Abstract
On the Android platform, apps make use of personal data as part of their business model, trading location, contacts, photos and more for app use. Few people are particularly aware of the permission settings or make changes to them. We hypothesize that both the difficulty in checking permission settings for all apps on a device, along with the lack of flexibility in deciding what happens to one's data, makes the perceived cost to protect one's privacy too high. In this paper, we present the preliminary results of a study that explores what happens when permission settings are more discretional at install time. We present the results of a pilot experiment, in which we ask users to negotiate which data they are happy to share, and we show that this results in higher user satisfaction than the typical take-it-or-leave-it setting. Our preliminary findings suggest negotiating consent is a powerful interaction mechanism that engages users and can enable them to strike a balance between privacy and pricing concerns.

Author Keywords
Interaction; Privacy; Negotiation; Mobile; Permissions

ACM Classification Keywords
H.5.2 [Information interfaces and presentation (e.g., HCI)]: User Interfaces - Interaction styles; K.4.1 [Computers and society]: Public Policy Issues - Privacy

Introduction

Concerns around the privacy and use of personal data by online services from web pages to smartphone apps have been expressed repeatedly in the media and research [1, 5, 7, 12, 19]. We know from related work in HCI that we very rarely read the terms and conditions relating to our private data, and even if we did take the time to read them, most of us would not understand [6, 11, 16, 17]. Once we are ready to make a decision, there is no opportunity to negotiate these terms, and often, we either need to accept the entire terms or forgo the service altogether. This consent situation becomes potentially even more problematic when we move from the desktop to the smartphone, when even more personal data becomes accessible, such as our photos, contacts, and text messages.

Smartphones follow a permission model that, in theory, helps safeguard the private data of their owners by selectively allowing data stored on the phone to pass through to others. However, while apps need some permissions for their functionality, the use of personal data is also often part of the app's business model, for example for showing targeted ads [15]. Moreover, users typically cannot selectively choose a set of permissions without severely hampering the app's functionality[1].

There is mounting evidence that current interaction mechanisms for consent are cracking at the seams. Consumers grow more and more weary of privacy-invasive and ad-heavy apps, as the soar of iOS's Adblocker recently showed [13]. Some users even take refuge in strategies for modifying Android's permission framework altogether, using root-based techniques [4, 20], reverse engineering procedures to remove permissions [8], and/or feeding apps mock data [3]. A continuation of the current situation is unlikely, not in the least because of upcoming (e.g. EU) regulations that will force services to take a more proactive approach towards privacy [18]. But services, in turn, can also expect to gain from a thorough re-evaluation of consent mechanisms, with the potential of bringing in consumers who are reluctant currently to adopt new technology due to privacy concerns [10, 11, 21].

Our work presented here intends to look at ways of how we might use new interaction paradigms to disrupt the cat-and-mouse privacy dynamics between developer and user, and to move forward from the binary take-it-or-leave-it, now-or-never approach that is called "consent" but is not meaningful. We explore a scenario where this binary distinction is more granular at purchasing time, so that people can interactively negotiate their permissions with their service in return for adaptive pricing. For example, the user may be comfortable granting an app access to their list of contacts, but will only share their text messages for a certain discount. By allowing a concurrent consenting dialogue to occur with the purchase of an app, the user can receive the app for an acceptable price and a personalized permission set that is deemed fair and reasonable.

To this end, we have developed an app that allows us to investigate whether negotiation is a helpful interaction mechanism for setting app permissions, enabling the user to make trade-offs between price and privacy concerns. Eventually, we intend for it to serve as a fruitful basis for evaluating forms of meaningful, automated consent. In an effort to make the setup as realistic as possible, we test users' responses to exposing their personal privacy-sensitive information contained within their own phone, combined with real monetary incentives to share their private data online.

[1] In iOS, and more recently in Android 5.0 (Marshmallow), users have access to a more granular permission manager; however, this interaction is still limited to binary, non-negotiable consent decisions.

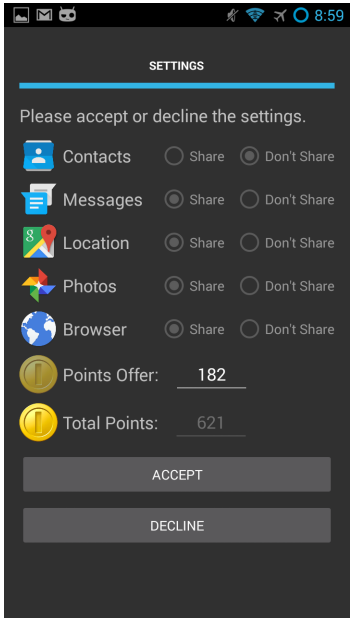

Figure 1: Settings interface for the take-it-or-leave-it treatment, in which users can only accept or decline the points offered based on preset preferences.

We have also performed a preliminary study comparing a negotiable permission set with a classic take-it-or-leave-it approach. Our preliminary findings suggest that negotiating consent is a viable interaction mechanism that engages users and empowers them in striking a balance between their concerns.

Interface Features

We developed the Meaningful Consent Android mobile application, which is an experimental tool in which users can receive monetary rewards in return for allowing their private data to be shared publicly over the internet. Users can set the app's privacy permissions to determine what type of personal smartphone data to share, depending on what the application is willing to offer them in return. The amount of data being shared affects the reward through the users' gain of points, which maps directly to monetary reward. The more users choose to share, the more points are available to them; this mirrors the situation of the app store providing discounts for sharing more private data.

We selected a set of permissions that are most often requested by apps [14] and could be mined as a data source (i.e., excluding permissions such as vibration and screen lock). This resulted in a set of five permissions, namely: access to the contact list, text messages, location, photos, and browsing history. The application includes two activities, settings and review, which are described below.

Settings Activity

In this activity, a number of privacy settings are shown to the user. These settings define the kind of data users are willing to share. Below that, the points on offer and the total points are displayed. The specific points offered can vary according to a predefined pricing scenario (detailed further below in the Procedure). We implemented two different designs for the setting activity:

Take-it-or-leave-it. This design (see Figure 1) aims to reflect today's situation prior to Android 6.0, in which people are required to accept all data access permissions requested by an app in order to proceed with the installation on their smartphone. Here, users can only accept or decline the privacy settings as determined by the app, and they receive a fixed amount of points for accepting. They are, however, able to retract this decision at a later stage (see Review Activity below).

Negotiation. The aim of this design (see Figure 2) is to allow users to negotiate the app's permissions to access their personal data. To do so, users can change the settings based on their privacy preferences, and receive a points offer for this setting by pressing the *Quote* button. Users can request multiple quotes, but each quote reduces the budget by 10 points to simulate service costs.

Review Activity

Once users have set their privacy permissions and accept the points on offer, the app collects a single randomly-selected, unique data point of each data type to which the user gave access. Following this, the Review Activity is initiated (see Figure 3), in which a user can see exactly what is being shared and can choose to retract access to any particular data.

The purpose of this activity is twofold. First, it makes users fully aware of the consequences of the selected privacy settings by making it concrete and meaningful to the user (as opposed to the more abstract permission settings). Second, it allows us to measure to what extent the choices from the settings stage were indeed meaningful and to compare dif-

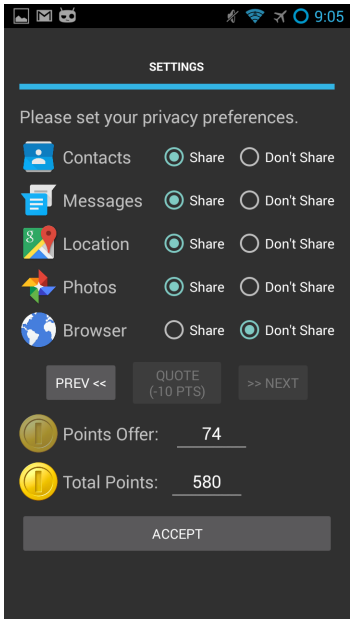

Figure 2: Settings interface for the negotiation treatment, in which users can modify preferences and are offered different point quotes.

ferent interaction designs (i.e. a design where users retract fewer permissions is arguably more meaningful).

Preliminary User Study

We conducted a preliminary pilot with the main purpose to investigate three key features:

User understanding of study procedure. We wanted to check that our study materials, the app itself, and indeed the more general study protocol, were understandable to participants and that they were aware of the choices that they were being asked to make. In particular, our experimental design requires that participants believe that their choices have genuine privacy consequences.

Appropriateness of selected data. We aimed to check if the app itself was reliable, and that the data sampling part of the app actually collected potentially sensitive information that would give participants reason to think twice about the potential consequences of publication.

Qualitative insight into participant reasoning. We wanted to gain initial insight into the decision making process of our participants. In particular, we were interested in what characteristics of the collected data, or possible consequences, are taken into account by participants as they evaluate whether or not they wish to share particular types of individual pieces of data.

Participants

We recruited 7 participants (3 female and 4 male) through personal contacts within the University of Southampton. Participants were all undergraduate or masters students studying different subjects (e.g., Film, English and Biomedical). Their age ranged from 18 to 25.

Procedure

To evaluate the app, we used a think-aloud study with individual participants who were asked to install and use the app. After collecting some basic demographic details, we asked each participant to make 12 permission decisions; 6 using the take-it-or-leave-it interface, and 6 using the negotiation interface.

Participants were informed, both through the information sheet and verbally by the investigator present, that any data they shared would be made available on a public website, as approved by our independent ethics committee. The participants were urged to think aloud as they used the app.

In order to elicit different responses according to the offered points, we presented the participants with different pricing scenarios, in which the combination of permissions was valued differently in terms of points. Participants experienced the same pricing scenarios in both designs. In each scenario, they interacted alternately with the Settings and Review activities.

Participants were told beforehand that they would be paid in cash based on their total amount of points (i.e., we follow the common practice of using experimental currency units [9]). After receiving the payment, the participants were debriefed about the study, stating its purpose in more detail and indicating that their data was never made publicly available on any website despite us telling them so.

Results

Appropriateness of Selected Data and Participant Responses

Participants actively engaged in the negotiation process, requesting between 4 and 11 quotes in total for their data. Each experiment lasted between 5 and 26 minutes, most of which the participants spent fine-tuning their decision-making. The users were also keen to review their data, and

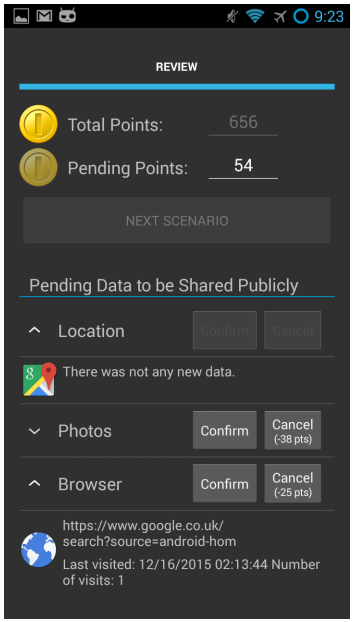

Figure 3: Review interface for both treatments, in which users can revise their personal data being shared, and confirm or withdraw the sharing process for each data type.

often retracted information that they elected to share earlier; the main retractions were observed in more sensitive data, namely contacts and photos (more details are given below). The app sampled a wide range of data during the experiments, with between 300 and 12000 potential data points available per participant.

SMS Messages. Most participants were not overly concerned about sharing text messages. They raised concerns over sharing texts containing particular pieces of information, like a telephone number, but these were quite rare and many participants suggested that the messages would be meaningless without the context of the conversation.

Location. For this in-lab study, rather than collecting GPS data from the location service itself, we attempted to extract it from photos on the device to get a wider range of past locations. However, 5 out of 7 participants had geotagging of their pictures disabled, and hence our insight into participants' feelings towards location data is limited.

Photographs. Most participants demonstrated some reservations over the sharing of photographs taken from their device. However, as explained in more detail below, most were happy to initially share and then revoke any photographs that they were unhappy with, with some reasoning that most photos on their device were fine, with only a minority containing content (for instance relatives, or friends' children) that they would not like to be published.

Contacts. Sharing contact data seems to elicit the most reluctance from participants. Most participants said that they felt they have no right to make decisions about other people's contact details, and so choosing to sell them is wrong. However, many participants were less reluctant to share the details of people who they do not know as well, or even dislike, especially when offered more points to do so.

Browsing History. Most participants raised no specific concerns regarding browsing history, and were generally happy to share it. However, some were concerned that this data could reveal what they had searched for. Most participants realized, after some trial and error, that most of the chosen URLs were not sensitive or even intelligible out of context.

Understanding of Study Procedures

During the debrief session, participants indicated that they believed their data would be shared online and, during the course of the study, they did seem to take it as given that their shared data might be seen by others. All participants received around £8 of a potential payment between £5 and £10. The participants were keen to change the default settings of the app and displayed a consistent preference for sharing certain types of data. This indicates that they were careful to balance between the monetary incentive and retaining their private data.

Discussion

We obtained four main insights into participant reasoning during the study, which, although preliminary due to the small user sample, stood out in particular.

Negotiation is preferred. When asked about which interaction style they preferred, all participants indicated that they preferred negotiation to the take-it-or-leave-it approach. This was typically due to its flexibility at adjusting permissions, causing the users to feel more in control.

Review is important. The protocol for this study presented the review screen as soon as a decision had been

made, allowing participants to immediately undo the sharing of their data. This seems to be reflected in participants' behavior. Many participants, after some initial trial and error, realized that even if a data type (e.g. photos) contained some highly sensitive material, the risk of this being chosen at random was low, and the possibility of immediate revocation further reduced this risk.

Stability of choices, regardless of price. After an initial learning phase, most participants adopted a behavior in which the permissions chosen in the negotiation condition were fairly static. Participants had a sense of which data they were happy to share (with the knowledge that they would be able to review) and this did not seem to be affected much, if at all, by the quotes that they received. Participants stated that although some permissions boosted the received points only marginally, some points are better than none (see below). For instance, one participant adopted a strategy of sharing all data, except for contacts, taking a single quote and accepting it immediately. In the take-it-or-leave-it condition, such behavior was manifested slightly differently; participants would typically accept any offer that did not request any "sensitive" data.

Little sense of intrinsic value. The behavior described above, as well as participants' verbal descriptions of how they were deciding to accept or reject offers, seems to suggest that participants have little sense of the intrinsic value of the data they were being asked to share, or even of the "cost" of sharing it. Some participants anchored on earlier prices, with statements such as: "This was worth more last time, I think I should reject this offer". We did observe that participants who were reluctant to share their sensitive data were sometimes more tempted to accept high-value offers. This points toward the possibility of finding the "value" of that data to an individual user, even if participants themselves do not necessarily seem to be manifestly aware of it in their reasoning.

Conclusion

While the work is at early stages, results are sufficiently encouraging to suggest that negotiation of consent is a viable interaction mechanism. The results offer support for the CHI community to have provisional confidence in further exploration of negotiation, not only for permissions around data sharing, but also for other models for deliberate consent. Based on our findings, the review screen (which is intended only as a measure) needs to be modified so that its influence on the decision making process can be better understood. We propose changing the retraction ability of the review stage into merely expressing "regret".

Although all participants preferred the negotiation setup over take-it-or-leave-it, we envisage some of the benefits of a take-it-or-leave-it interface to become apparent in scenarios where time pressure is greater or the sharing action itself is not the main focus of the users' attention. We also expect to obtain insight into the market value of permissions with a more substantial range of pricing scenarios and an extended study duration, as we found that the willingness to pay is a process learned and stabilizing over time. The long term challenge here is to see if artificial intelligence techniques can help support the user in their negotiation decisions along the lines of [2], and whether this can lead to a formulation of meaningful, automated consent.

Acknowledgements

This work was supported by the EPSRC, grant number EP/K039989/1. Ilaria Liccardi was supported by the European Commission Marie Curie International Outgoing Fellowship grant 2011- 301567 Social Privacy.

REFERENCES

1. Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. 2015. 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 (CHI '15)*. ACM, New York, NY, USA, 787–796. DOI: http://dx.doi.org/10.1145/2702123.2702210
2. Tim Baarslag, Ilaria Liccardi, Enrico H. Gerding, Richard Gomer, and M.C. Schraefel. 2015. Negotiating Mobile App Permissions. In *Amsterdam privacy conference*. http://eprints.soton.ac.uk/377378/
3. Alastair R Beresford, Andrew Rice, Nicholas Skehin, and Ripduman Sohan. 2011. Mockdroid: trading privacy for application functionality on smartphones. In *Proceedings of the 12th Workshop on Mobile Computing Systems and Applications*. ACM, 49–54.
4. M. Bokhurst. 2015. XPrivacy. (2015). https://github.com/M66B/XPrivacy
5. Ramnath K. Chellappa and Raymond G. Sin. 2005. Personalization Versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. *Inf. Technol. and Management* 6, 2-3 (April 2005), 181–202. DOI: http://dx.doi.org/10.1007/s10799-005-5879-y
6. Emma Cradock, David Millard, and Sophie Stalla-Bourdillon. 2015. Investigating Similarity Between Privacy Policies of Social Networking Sites As a Precursor for Standardization. In *Proceedings of the 24th International Conference on World Wide Web (WWW '15 Companion)*. International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, Switzerland, 283–289. DOI: http://dx.doi.org/10.1145/2740908.2743050
7. Molly Crain. 2015. The biggest myth about phone privacy. (2015). http://www.bbc.com/future/story/20150206-biggest-myth-about-phone-privacy
8. Quang Do, B. Martini, and K.-K.R. Choo. 2014. Enhancing User Privacy on Android Mobile Devices via Permissions Removal. In *System Sciences (HICSS), 2014 47th Hawaii International Conference on*. 5070–5079. DOI: http://dx.doi.org/10.1109/HICSS.2014.623
9. Andreas Drichoutis, Jayson Lusk, Rodolfo Nayga, and others. 2013. The veil of experimental currency units. *Munich Personal RePEc Archive (MPRA) Paper No* 46906 (2013).
10. Mauricio S. Featherman and Paul A. Pavlou. 2003. Predicting e-services adoption: a perceived risk facets perspective. *International Journal of Human-Computer Studies* 59, 4 (2003), 451 – 474. DOI: http://dx.doi.org/10.1016/S1071-5819(03)00111-3 Zhang and Dillon Special Issue on {HCI} and {MIS}.
11. Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android Permissions: User Attention, Comprehension, and Behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12)*. ACM, New York, NY, USA, Article 3, 14 pages. DOI: http://dx.doi.org/10.1145/2335356.2335360
12. Glenn Greenwald. 2014. Why privacy matters. (2014). http://www.ted.com/talks/glenn_greenwald_why_privacy_matters

13. Alex Hern. 2015. iOS 9 adblocker apps shoot to top of charts on day one. (2015). http://www.theguardian.com/technology/2015/sep/17/adblockers-ios-9-app-charts-peace
14. Ilaria Liccardi, Joseph Pato, and Daniel J Weitzner. 2014a. Improving User Choice Through Better Mobile Apps Transparency and Permissions Analysis. *Journal of Privacy and Confidentiality* 5, 2 (2014), 1.
15. Ilaria Liccardi, Joseph Pato, Daniel J. Weitzner, Hal Abelson, and David De Roure. 2014b. No Technical Understanding Required: Helping Users Make Informed Choices About Access to Their Personal Data. In *Proceedings of the 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MOBIQUITOUS '14)*. ICST, ICST, Brussels, Belgium, Belgium, 140–150. DOI:http://dx.doi.org/10.4108/icst.mobiquitous.2014.258066
16. Ewa Luger, Stuart Moran, and Tom Rodden. 2013. Consent for All: Revealing the Hidden Complexity of Terms and Conditions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*. ACM, New York, NY, USA, 2687–2696. DOI: http://dx.doi.org/10.1145/2470654.2481371
17. Aleecia M. Mcdonald, Robert W. Reeder, Patrick Gage Kelley, and Lorrie Faith Cranor. 2009. A Comparative Study of Online Privacy Policies and Formats. In *Proceedings of the 9th International Symposium on Privacy Enhancing Technologies (PETS '09)*. Springer-Verlag, Berlin, Heidelberg, 37–55. DOI: http://dx.doi.org/10.1007/978-3-642-03168-7_3
18. European Parliament. 2015. Article 29 Data Protection Working Party. (2015). http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/index_en.htm
19. Malte Spitz. 2015. Your phone company is watching. (2015). https://www.ted.com/talks/malte_spitz_your_phone_company_is_watching
20. R. Vollmer. 2015. Xposed framework. (2015). http://repo.xposed.info/
21. Tao Zhou. 2011. The impact of privacy concern on user adoption of location-based services. *Industrial Management & Data Systems* 111, 2 (2011), 212–226. DOI:http://dx.doi.org/10.1108/02635571111115146