Negotiating Mobile App Permissions

Tim Baarslag 1 , Ilaria Liccardi 2,3 , Enrico H. Gerding 1 , Richard Gomer 4 and m.c. schraefel 1,2

Affiliations: *1* Agents, Interaction and Complexity Group, University of Southampton, UK.
2 CSAIL, Massachusetts Institute of Technology, USA.
3 Oxford eResearch
Center, University of Oxford, UK.
4 Web and Internet Science Group, University of Southampton, UK.

Abstract

When people install an Android app on their smartphone, they are required to accept all permissions requested by the app in order to proceed with installation. That is, the consent mechanism of the app market limits the user to a binary decision: either *t ake it, or leave it.* However, there is often little to no information about the *p urpose* for accessing this information, with apps often requesting permissions that have little to do with the app and are used only for advertising purposes [5]. For instance, an app might not need location data but might still require access in order to run (a common example [8] is Angry birds by Rovio). In previous research it was found that only 7% of apps presented a privacy policy within the app's page [2]. These policies are often long, full of legal terminology, and are hard to read on a small screen.

Furthermore, people are often unaware that apps may collect their personal data [3] due to the fact that the permission mechanisms are often difficult to understand [9] and that part of this collection happens silently in the background [6]. When users are made aware of this collection, they feel much less willing to share those data which they perceive be extremely sensitive [4,9]. Some express shock and a desire to remove the app [7,8] or experience a sense of "creepiness" that results in a loss of trust [11].

The perceived sensitivity of data is often personal and can also vary within the individual's *c ontext* [10,12]. For example, a user might be willing to share when he or she is at a certain location or while engaging in a certain activity (e.g. relaxing), but not when performing another (e.g. working). It is impossible to consent to the collection of data for every foreseeable purpose, given the incomplete, missing or difficult to understand information [9] users receive when making the decision about whether to install an app.

Another critical problem is posed by *timing* : a person is asked at the time of purchase to make potentially complex decisions about whether to allow access. This may be too cognitively complex in the context of undertaking a broader task, or in environments that place other demands on the person's attention.

To address each of these issues, we propose a design in which the user can negotiate the app's permissions to access their personal data. For example, users who prefer not to view ads could opt to pay an additional fee for this, as is currently offered within certain apps such as "Cut the Rope".

However, negotiating with each app might be cumbersome and difficult to achieve by users. H ence, to make this process easier, we propose an approach that uses an agentbased framework that employs software agents to represent users in their privacy negotiation with the app in an automated manner [13,14].

Negotiation allows for every permission to be agreed upon separately, leading to a more finegrained solution that is acceptable, reasonable and meaningful for both parties. This way, users are able to obtain a customized data contract that respects their privacy preferences, while app developers may get a sale from otherwise hesitant users, with an increase in trust, higher customer satisfaction, and consent that is more meaningful – and possibly at a higher revenue than expected. For granularity of context, the agent interaction enables both the developer and the purchaser to negotiate an acceptable deal for services that may include both contextsensitive data and price or no deal. For timing, the policy with which the agent engages an app can be set well in advance of any purchase, and refined with the user at appropriate and scheduled times for review not unlike reviewing insurance or bank statements. We see this approach as a winwin opportunity for both developers and purchasers as well as providing a new opportunity for app stores to act as a negotiation hub.

References

[1] Acquisti, A.,and Grossklags, J.Privacy and rationality in individual decision making. *S ecurity Privacy, IEEE* (2005), 26–33.

[2] I. Liccardi, J. Pato, and D. J. Weitzner. Improving Mobile App selection through Transparency and Better Permission Analysis. *J ournal of Privacy and Confidentiality: Vol. 5: Iss. 2, Article 1.* , pages 1–55, 2014.

[3] PorterFelt, A., Egelman S., Wagner. D, I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns. In *Proc. of ACM SPSM '12* , pages 33–44, 2012.

[4] Bansal, G., Zahedi, F., Gefen, D., et al.The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *D ecision Support Systems 49* , 2 (2010), 138–150.

[5] P. Pearce, A. P. Felt, G. Nunez, and D. Wagner. Addroid: privilege separation for applications and advertisers in android. In *Proc. of ACM ASIACCS '12* , pages 71–82, 2012.

[6] F. Zhang. Assessing intrusiveness of smartphone apps. Master's thesis, MIT, 2012.

[7] R. Balebako, J. Jung, W. Lu, L. F. Cranor, and C. Nguyen. "little brothers watching you": raising awareness of data leaks on smartphones. In *Proc. of ACM SOUPS '13* , pages 12:1–12:11, 2013.

[8] J. Lin, S. Amini, J. I. Hong, N. Sadeh, J. Lindqvist, and J. Zhang. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In *P roc. of ACM UBICOMP '12* , pages 501–510, 2012.

[9] Liccardi, I., Pato, J., Weitzner, D.J., Abelson, H., and DeRoure, D. No technical understanding required: Helping users make informed choices about access to their personal data. In *P roc. ACM Mobiquitous* (2014), 140–150.

[10] A hern, S., Eckles, D., Good, N. S., King, S., Naaman, M., and Nair, R. Overexposed?: Privacy patterns and considerations in online and mobile photo sharing. In *Proc. ACM CHI* (2007), 357–366.

[11] Shklovski, I., Mainwaring, S.D., Skúladóttir, H.H., and Borgthorsson, H. Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. In *Proc. ACM CHI* (2014), 2347–2356.

[12] S hih F., Liccardi I., Weitzner D.J., *P rivacy Tipping Points in Smartphones Privacy Preferences* , ACM SIGCHI Conference on Human Factors in Computing Systems 2015 (CHI), pp. 110
.

[13] Mitchell, Alan, Iain Henderson, and Doc Searls. Reinventing direct marketing—with VRM inside. *Journal of Direct, Data and Digital Marketing Practice* 10.1 (2008): 315.

[14] Gomer, Richard Charles, schraefel, m.c. and Gerding, Enrico (2014) Consenting agents: Semiautonomous interactions for ubiquitous consent. In *UbiComp'14 Workshop: How Do You Solve a Problem like Consent?, Seattle, US, 13 17 Sep 2014.* ACM, 653658.