Short Paper: Initial Recommendations for the Design of Privacy Management Tools for Smartphones

Alessandro Carelli, Matt Sinclair, Darren Southee

Short paper: initial recommendations for the design of privacy management tools for smartphones

Dr Alessandro Carelli [1] and Dr Matt Sinclair [2] and Dr Darren Southee [3]

[1,2,3] Loughborough Design School, Epinal Way, Loughborough (UK), UKLE11 3TU
a.carelli@lboro.ac.uk

Abstract. The continuing rise in the popularity of smartphones has led to an accompanying rise in the exposure of users to privacy threats as in the case of unintended leakage of personal information from apps. To improve transparency and the ability of users to control data leakage, the design of privacy-enhancing tools aimed at reducing the burden of informed privacy-decisions should be grounded upon users' tacit needs and preferences. To this end, the present study explores users' personal perception and concerns toward privacy and their expectations. Initial recommendations include: (1) consideration of the preferences of users for preserving functionalities of their apps, informing users about both (2) the real benefits and actual possibility of using privacy management tools and (3) suspected applications' data collection behaviours in a way that matches their real concerns and values.

Keywords: Privacy, Human-Centered Design, Smartphones, Privacy-enhancing technology, user experience

1 Introduction

While the popularity of the smartphone continues to be a growing phenomenon worldwide [1], such devices also pose accompanying privacy threats to users, as in the case of personal information leaked by apps without users' full awareness or consent [2].

Diverse studies have pointed out how personal data leaked online represents a threat which is far more concerning than simply annoying users with invasive advertisements and potentially affecting the social life of individuals [3]. Among the potential implications for privacy there is the risk that leaked data could be used to (1) uniquely identify users without referring to their name and physical address; (2) track users across different applications and devices; (3) build a comprehensive profile on individual users which can be used to predict behaviour and make decisions affecting services such as the provision of credit or used for online political microtargeting [3–6, 6–9].

Previous studies have highlighted different causes of application privacy mismanagement such as the general unawareness of data sharing, the preference of users to trade-off privacy for the benefit of using an app, and the complexity of the

system of permissions [10–13]. Thus, to enhance transparency and improve privacy users should be better supported through appropriate tools.

For this reason the present article is part of a broader research effort aiming at providing appropriate guidelines to design teams to help them improve the effectiveness and user experience of such tools.

2 Background

A number of contributions have addressed the potential of machine learning techniques to assist users in setting the privacy of their mobile devices through recommendations and automatic decisions [14–16]. Furthermore, [17], [18] and [19] provided usability recommendations for browser extensions blocking online behavioural tracking and summarized in Table 1.

Table 1. Summary of design recommendations for browser extensions blocking online behavioural tracking from [17], [18] and [19]

Guideline	Reference
Users want protections that don't break the functionality of the web pages and online service they use	[19]
The system (i.e. the online browser) should protect users automatically and be designed in a way that reduces the chance that the breakages occur	[17]
Users should be better informed about why web trackers are present, the information they are collecting and how it might be used	[18]
An indication of the privacy risks is likely to improve the meaningful of the information as well as the use of icon colour can inform users about critical situations such as when blocking may break the website's functionality. Furthermore, the information provided by the tools should be relevant and actionable for users	[18]
Setup materials which include videos and tutorials are useful to shape users' mental models and to increase the trust toward the privacy-enhancing extension	[18]

However, no previous study has focused specifically on the user experience of privacy management tools for smartphones, or offered guidelines for improving their design.

Furthermore, although user experience and Human-centred design are concepts widely accepted within the HCI community [20], understanding the experience of users with privacy and security technologies is a relatively new area of research. In this connection [20–23] indicated the importance of extending inquiry to the experiential

aspects of privacy technologies, as users have values and tacit needs which may remain underrepresented if not appropriately considered.

In order to address this gap, this research has inquired into users' personal perceptions of privacy and their expectations towards a privacy management app, in order to derive recommendations for designers.

3 Study design

3.1 Sample

The study involved an opportunity sample of nine participants recruited from the researchers' personal network and university mailing list from both Italy and UK, over a period of 18 weeks. The average age of participants was 29, in a range of ages from 23 to 34 years; eight participants had an advanced degree and one a bachelor's degree. Only one participant held a degree in computer science since priority was given to 'typical users' with no IT background and thus represented the primary focus of a PMT as understood in this article. This represents the first part of an ongoing research project investigating the users' subjective experiences while using a privacy management app.

3.2 Procedure

Participants were required to answer semi-structured questions and to think-aloud while using the interview materials. Such material included a set of interview boards aiming at helping participants elaborate their thoughts, and MyPermissions (MP), a popular privacy management app which enables smartphone users to manage the privacy settings of third party apps installed on smartphones which participants were required to install and use on their own smartphone (Figure 1).

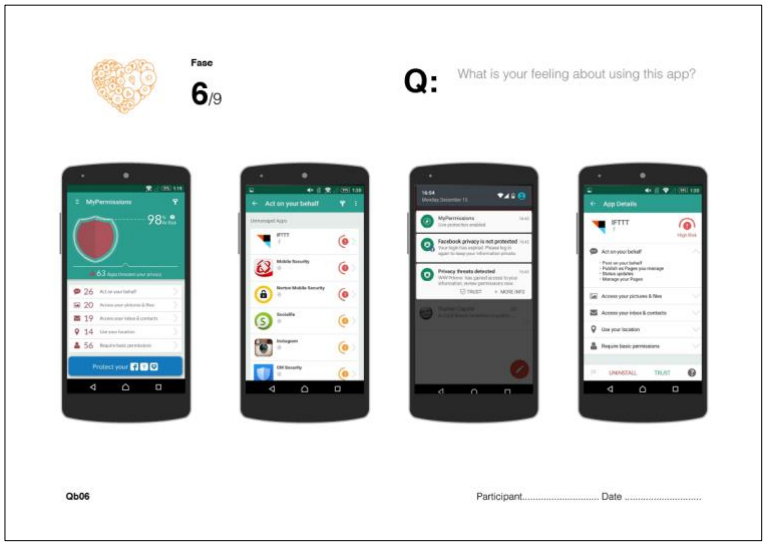

Fig. 1. A printed board used throughout the interview showing MyPermissions' screenshots.

Asking users to think-aloud while interacting with a technology or performing other tasks is a common method in usability and user experience research, as it allows researchers to probe participants' mental models, uncertainties and misconceptions [24, 25]. During the interview participants were required to think aloud while using both the interview boards and the MP app, allowing the researcher to probe further their thoughts were appropriate.

In order to understand the personal perceptions of privacy and expectations of users towards a privacy management app, questions covered the following topics:

- 'Breaking the ice' and understand participants' attitude toward smartphone
- Comprehend participants' attitude toward app privacy
- Collect opinions about, and previous experience with, privacy management tools
- Probe participants' expectations toward MP

Such topics were grounded upon recommendations in [20] which suggests to probe user's practices, subjective meanings and the fit of privacy technologies in to user's everyday lives.

Interviews were conducted individually with each participant and lasted 100 minutes on average. After a break-the-ice question where participants described apps they frequently use, they were asked to reflect upon the fit of their smartphone and apps into their everyday lives by placing their smartphone in a value-based scale from 'fundamental' to 'not essential', and provide explanations. This value-based scale, which was used with the solely scope of collecting qualitative data, was informed by the survey on smartphone ownership carried out by [26] which pointed out how smartphones are being increasingly embedded in the daily lives in particular of people in the age range 18-29.

As a second task, participants were asked about their subjective perceptions of security or privacy, using their own words. This task was also intended to understand their real knowledge and perception of potential privacy threats related to smartphones and applications. The interview then moved on to asking participants about the typologies of data potentially leaked by apps, as well as the reasons, modalities and potential recipients of the data sharing.

As a third task, participants were first required to use their phone to check the permissions and privacy notes of a popular weather forecasting app and to discuss whether they were informative. Participants were then asked to express their expectations toward MP. No participants were aware of MP before entering the study, thus participants were first introduced to the app's trailer, which did not show the application's function in detail but rather metaphorically depicted the role of MP[1]. Then, participants were shown a board with screenshots of UIs of MP to better articulate their thoughts.

Finally, participants were required to install MP on their smartphone and to think aloud while freely exploring the information provided by MP on the app installed on their smartphones.

Interviews were transcribed verbatim and analysed by the author through an iterative open thematic approach aimed at identifying and organising relevant themes from the text. Before proceeding with the axial coding transcripts were firstly analysed inductively to avoid biasing the findings with the researcher's pre-assumption. The analysis of data was performed using MaxQDA, a Computer Assisted Qualitative Data Analysis (CAQDA) software following the guidelines suggested in [27]. Throughout the process of analysis the emerging themes and sub-themes were visualised using the dendogram representation feature available on the CAQDA. Due to space constraints the summary of the emerging themes is available upon request.

4 Findings

Many of the findings confirmed other studies of attitudes toward mobile privacy and smartphone data leakage.

4.1 Smartphones, privacy information and control features

Participants were split regarding how fundamental their smartphone was to everyday life. As in [28], for five participants who perceived their smartphone as fundamental, such devices became an extension of the self which may lead to the experiencing of stress and anxiety when deprived of their device. As in [26], despite the divergence of opinions reported above, all participants experienced a range of conflicts concerning phone ownership which range from being exposed to undesired privacy exposition to continuous distractions.

[1] The trailer of MyPermission app shown to participants is available at this link: https://www.youtube.com/watch?time_continue=1&v=fTiPigYxxHE

"I feel ashamed that everything is based on the phone but I cannot escape […] it is shamed to be based on the phone, to a machine to be happy" — P4

One participant also reported relying on their smartphone in specific situations such as while living in a foreign country, as well as simplifying their access to public services in the specific case of the UK. Such context-dependent reliance on smartphones shows how the flexibility of such devices, along with the growing number of situations in which they are used, make them deeply integrated into people's everyday lives.

As in [15], [12] and [29], participants were in general not familiar, or generally did not pay particular attention to, privacy information and control points such as the Privacy policy and the list of permissions which was hidden within the settings menu.

4.2 Personal perception and concerns toward privacy

As reported in [18], all participants were generally aware and concerned about different privacy-invasive activities of their apps. Nevertheless as in [22] and [21], four participants consciously accepted the trade-off in order to keep using their relevant apps and services.

"So it's easy to close your eyes [from the] bad things they can do with your data, not necessarily bad but things that you don't want them to do with your data." — P8

However, five participants reported they were generally not entirely passive with regard to being exposed to privacy violations, and support the findings of [30] in reporting engagement in diverse, non-technical coping strategies to reduce the unintended collection of their private information. Examples of this include the denying of storing personal information for future use by digital marketplaces, and self-moderated information disclosure on social media and while using instant message apps.

Seven participants showed a strong awareness about the trade-off concerning the use of mobile apps, which is in some disagreement with [11]. Together with the general rise in the level of concern towards the sharing of personal information online [31], this discrepancy may also be accounted for by the higher level of education of the sample. Furthermore, when probed about their subjective understanding of personal information, seven participants associated personal information with traits of participants' personal identity such as personal views and opinions, political ideas as well as information on habits and daily routines.

"I would probably described it as something as intimate, that I would only want to share with certain people at certain time" — P9; Interview 1.

All participants were able to identify a wide range of personal information types that could be stored on their phones, with seven reporting having inferred these information

types from indirect feedback, contextual cues and reflecting on their direct experience while using their apps. However, participants were generally unsure about which could be shared more frequently by their apps. Similarly to [31], location, photos and email address were among the personal information items that could be potentially shared more frequently by apps according to participants. Furthermore, as in [11] six participants admitted in particular of having had difficulties understanding how data could have been disclosed by their apps while the others were generally unsure.

4.3 Expectations toward MP

As in [11, 22, 32], six participants expected MP to fulfill their interest toward the opaque data sharing mechanisms taking place inside their smartphones, as well enhancing transparency and control.

> *"So it would be good to now for each app [...] what they actually know about you" — P8; Interview 1.*

Probed further about the features they would expect from MP, participants' answers showed misconceptions toward the scope of a privacy management app and the role of permissions. For instance, one participant mentioned deleting online footprints after a certain time and another participant described using apps without allowing permissions, which would impede the app's ability to function.

Finally, it may be tempting to interpret the desire for enhancing autonomy, freedom of choice and awareness expressed by participants as the consequence of their general understanding and frustration toward application data leakage. Indeed, they believed that data collection from apps is being voluntarily prosecuted with intended secrecy, in a way that excludes them and offers no chance to be consciously involved in the trade-offs of their privacy. Users are concerned about the asymmetry of power between themselves and the service providers, and fear that the huge amount of information taken from them may be employed to affect their decisional autonomy, as well as other unintended uses. Users therefore value the chance of enhancing their awareness of data sharing and to have more opportunities to intervene in the trade-off between privacy and functionalities underlying the use of their smartphones.

5 Discussion and initial recommendations

Given the growing importance of smartphones in daily life and the difficulties in tackling the related privacy issues, privacy management apps would play a crucial role in improving users' privacy.

This research was undertaken using an experiential-based inquiry which allowed researchers to understand personal perceptions of privacy and expectations toward the technology, and to ground the initial recommendations on such insights. In particular, the research allowed the revealing of participants' hidden practices, subjective meanings of privacy, and expectations toward the privacy management technology. As pointed out by [20], successful technologies are those which are able to "respond

sensibly to the needs and values of users, and are not necessarily those that are the most usable" [20:83]. Considering the above insights, three main initial recommendations to enhance the transparency, reliability and user experience of such apps can be derived.

Firstly, privacy-enhancing tools should show consideration of the preferences of users for preserving functionalities of their apps. Participants showed awareness and concern toward different privacy-invasive activities concerning their apps and as in [22] consciously accepted the trade-off in order to keep using their relevant apps and services. Despite this, and as also reported in [30] , they were generally not entirely passive with regard to being exposed to privacy violations, engaging in non-technical coping strategies to reduce the unintended exposition of their private information. Privacy management tools should therefore support users in finding a balance between the need for privacy the need to keep the relevant functionalities of their apps and services.

Secondly, privacy-enhancing tools should correctly inform users about the real benefits and actual possibility of using privacy management tools to enhance privacy of mobile applications. Users may not be familiar with the specific functions performed by privacy-enhancing technologies. Furthermore, as attitudes and expectations affect the users' intention to adopt a new piece of technology [33, 34], misconceptions held about the role of a privacy management tools is likely to lead to a mismatch between users' expectations, reducing their willingness to adopt the tool if these expectations are not managed.

Finally, greater effort is required from both design researchers and practitioners in order to inform users about suspected applications' data collection behaviours in a way that matches their real concerns and values. The association of personal information with traits of personal identity has interesting design implications. In particular, research suggests that the lack of cognitive and emotional understanding between users and their data suggested in [21] and [22] can be motivated by the difficulty of understanding the outcomes of the processing of such data. Indeed, as pointed out by [35], the connection between apparently innocuous data types and their use to infer more sensitive information is likely to be hard to understand by average users who do not have an extensive understanding of the matter. Thus designers must find ways to make such connection more explicit and in so doing reducing such a cognitive and emotional gap.

While the first recommendation has been partially covered in [19], who reported that users want protections that don't break the functionality of the web pages and online services they use, the other two recommendations have not been mentioned in previous studies.

Overall, the above recommendations represent a first attempt to derive recommendations for the design of PMTs for smartphones, grounded on the analysis of subjective meanings and perceptions of privacy and technology. In so doing, this research has contributed to the growing stream of research focused on the experience of privacy and security. Furthermore, in adopting the discursive approach described in section 3.2 it provided complementary insights compared to those coming from studies focused on usability as in [17], [18] and [19]. The potential of such an approach is that

of leveraging Human-Centred Design practices to design privacy technologies which are more adherent to the values and needs of users.

5.1 Limitations and future work

One limitation of the in-depth qualitative investigation reported in this article is that the small sample of relatively young and well-educated participants does not allow generalisation across a wide population of users.

However, studies enrolling a small number of participants are not uncommon in practice-based research [36–39] as they intend to provide a richer descriptive understanding of the unknown design space which can inform reserachers about salient issues for future research and practices. Furthermore, the figure on smartphone ownership offered by [1], shows that in the UK people in the age groups 16–24 and 25–34 regard smartphones as the most important device for internet access, suggesting that the targeted group is indeed representative of a relevant segment of the real population.

Nonetheless, one way in which this limitation may have affected the reported findings is the general high level of awareness of data leakage reported by participants, which may be accounted for by the higher level of education of the sample. Therefore, future study may consider the involvement of a more heterogeneous sample which is representative of a wider age range groups, and different level of instructions.

Finally, as pointed out by [20], future research may also engage with groups with specific needs as it is likely that a challenging group of users can offer insights which are potentially beneficial for the wider population.

6 Conclusions

This study used both semi-structured interviews and required users to think-aloud while going through the proposed tasks to investigate users' personal perceptions and concerns towards smartphone privacy, and their expectations concerning a privacy management app. The findings were discussed in the light of those reported in the relevant literature.

To improve the design of privacy-enhancing tools for smartphones it has been recommended to (1) explore ways to support users to find the appropriate balance among privacy and functionality; (2) appropriately informing users about the real benefits and possibility of the tool and (3) further exploring the emotional and cognitive gap concerning leaked information.

To further extend the proposed set of initial recommendations, in the next step of the study design probes will be used to reveal users' experience of the privacy management app during a prolonged in-situ trial period.

References

1. Ofcom. *The Communications Market Report*. ofcom, https://www.ofcom.org.uk/__data/assets/pdf_file/0017/105074/cmr-2017-uk.pdf (3 August 2017, accessed 7 May 2018).
2. Zang J, Dummit K, Graves J, et al. Who Knows What About Me? A Survey of Behind the Scenes Personal Data Sharing to Third Parties by Mobile Apps. *Technology Science*, http://techscience.org/a/2015103001/ (2015, accessed 28 November 2015).
3. Book TR. *Privacy Concerns in Android Advertising Libraries*. Thesis, https://scholarship.rice.edu/handle/1911/87711 (2015, accessed 21 January 2016).
4. Narayanan A, Shmatikov V. Myths and Fallacies of 'Personally Identifiable Information'. *Commun ACM* 2010; 53: 24–26.
5. Christl W, Spiekermann S. *Networks of Control*, http://www.facultas.at/list?isbn=9783708914732 (2016, accessed 10 October 2016).
6. Zuiderveen Borgesius F. *Singling Out People Without Knowing Their Names – Behavioural Targeting, Pseudonymous Data, and the New Data Protection Regulation*. SSRN Scholarly Paper ID 2733115, Rochester, NY: Social Science Research Network, https://papers.ssrn.com/abstract=2733115 (16 February 2016, accessed 3 May 2018).
7. Schiff A. 2015 Edition: A Marketer's Guide To Cross-Device Identity. *AdExchanger*, https://adexchanger.com/data-exchanges/a-marketers-guide-to-cross-device-identity/ (2015, accessed 31 August 2018).
8. de Montjoye Y-A, Hidalgo CA, Verleysen M, et al. Unique in the Crowd: The privacy bounds of human mobility. *Scientific Reports*; 3. Epub ahead of print 25 March 2013. DOI: 10.1038/srep01376.
9. Borgesius FJZ, Möller J, Kruikemeier S, et al. Online Political Microtargeting: Promises and Threats for Democracy. *Utrecht Law Review*; 14. Epub ahead of print 9 February 2018. DOI: 10.18352/ulr.420.
10. Almuhimedi H, Schaub F, Sadeh N, et al. 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*. New York, NY, USA: ACM, pp. 787–796.
11. Balebako R, Jung J, Lu W, et al. 'Little Brothers Watching You': Raising Awareness of Data Leaks on Smartphones. In: *Proceedings of the Ninth Symposium on Usable Privacy and Security*. New York, NY, USA: ACM, pp. 12:1–12:11.
12. Felt AP, Egelman S, Wagner D. I've Got 99 Problems, but Vibration Ain't One: A Survey of Smartphone Users' Concerns. In: *Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*. New York, NY, USA: ACM, pp. 33–44.
13. [13] Lin J, Amini S, Hong JI, et al. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In: *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*. ACM, pp. 501–510.
14. Liu B, Andersen MS, Schaub F, et al. Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions. In: *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. Denver, CO: USENIX Association, pp. 27–41.
15. Tsai L, Wijesekera P, Reardon J, et al. Turtle Guard: Helping Android Users Apply Contextual Privacy Preferences. In: *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. Santa Clara, CA: USENIX Association, pp. 145–162.
16. Wijesekera P, Baokar A, Tsai JY, et al. *The Feasibility of Dynamically Granted Permissions: Aligning Mobile Privacy with User Preferences*. 2017.

17. Mathur A, Vitak J, Narayanan A, et al. Characterizing the Use of Browser-Based Blocking Extensions To Prevent Online Tracking - Semantic Scholar, /paper/Characterizing-the-Use-of-Browser-Based-Blocking-To-Mathur-Narayanan/aaa49be6c2860e60e340dc55793fc3d5e9f7b541 (2018, accessed 27 July 2018).
18. Schaub F, Marella A, Kalvani P, et al. Watching Them Watching Me: Browser Extensions Impact on User Privacy Awareness and Concern. 2016. Epub ahead of print 1 January 2016. DOI: 10.14722/usec.2016.23017.
19. Leon P, Ur B, Shay R, et al. Why Johnny Can'T Opt out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York, NY, USA: ACM, pp. 589–598.
20. Dunphy P, Vines J, Coles-Kemp L, et al. Understanding the Experience-Centeredness of Privacy and Security Technologies. In: *Proceedings of the 2014 Workshop on New Security Paradigms Workshop*. New York, NY, USA: ACM, pp. 83–94.
21. Stark L. The emotional context of information privacy. *The Information Society* 2016; 32: 14–27.
22. Shklovski I, Mainwaring SD, Skúladóttir HH, et al. Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use. In: *Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems*. New York, NY, USA: ACM, pp. 2347–2356.
23. Mathiasen NR, Bødker S. Experiencing Security in Interaction Design. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York, NY, USA: ACM, pp. 2325–2334.
24. Nørgaard M, Hornb\a ek K. What Do Usability Evaluators Do in Practice?: An Explorative Study of Think-aloud Testing. In: *Proceedings of the 6th Conference on Designing Interactive Systems*. New York, NY, USA: ACM, pp. 209–218.
25. Olmsted-Hawala EL, Murphy ED, Hawala S, et al. Think-aloud Protocols: A Comparison of Three Think-aloud Protocols for Use in Testing Data-dissemination Web Sites for Usability. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York, NY, USA: ACM, pp. 2381–2390.
26. Smith A. *U.S. Smartphone Use in 2015*, http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/ (1 April 2015, accessed 4 April 2016).
27. Denscombe M. *The Good Research Guide*. Open University Press, 2007.
28. Clayton RB, Leshner G, Almond A. The Extended iSelf: The Impact of iPhone Separation on Cognition, Emotion, and Physiology. *Journal of Computer-Mediated Communication* 2015; 20: 119–135.
29. Kelley PG, Consolvo S, Cranor LF, et al. A Conundrum of Permissions: Installing Applications on an Android Smartphone. In: Blyth J, Dietrich S, Camp LJ (eds) *Financial Cryptography and Data Security*. Springer Berlin Heidelberg, pp. 68–79.
30. Rainie L, Madden M. *Americans' Privacy Strategies Post-Snowden*, http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/ (16 March 2015, accessed 18 March 2015).
31. Rainie L, Kiesler S, Kang R, et al. Part 2: Concerns About Personal Information Online. *Pew Research Center: Internet, Science & Tech*, http://www.pewinternet.org/2013/09/05/part-2-concerns-about-personal-information-online/ (2013, accessed 27 November 2017).
32. Jung J, Han S, Wetherall D. Short Paper: Enhancing Mobile Application Permissions with Runtime Feedback and Constraints. In: *Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*. New York, NY, USA: ACM, pp. 45–50.

33. Oinas-Kukkonen H, Harjumaa M. Persuasive Systems Design: Key Issues, Process Model, and System Features. *Communications of the Association for Information Systems*; 24, http://aisel.aisnet.org/cais/vol24/iss1/28 (2009).
34. Wright P (Peter C, McCarthy JC. *Experience-centered design designers, users, and communities in dialogue*. San Rafael, Calif.]: Morgan & Claypool, 2010.
35. Abrams M. *The Origins of Personal Data and its Implications for Governance*. SSRN Scholarly Paper ID 2510927, Rochester, NY: Social Science Research Network, https://papers.ssrn.com/abstract=2510927 (21 March 2014, accessed 16 January 2018).
36. Gaver WW, Bowers J, Boucher A, et al. The Drift Table: Designing for Ludic Engagement. In: *CHI '04 Extended Abstracts on Human Factors in Computing Systems*. New York, NY, USA: ACM, pp. 885–900.
37. Hutchinson H, Mackay W, Westerlund B, et al. Technology Probes: Inspiring Design for and with Families. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York, NY, USA: ACM, pp. 17–24.
38. Uriu D, Odom W. Designing for Domestic Memorialization and Remembrance: A Field Study of Fenestra in Japan. In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: ACM, pp. 5945–5957.
39. Vines J, Blythe M, Dunphy P, et al. Cheque Mates: Participatory Design of Digital Payments with Eighty Somethings. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York, NY, USA: ACM, pp. 1189–1198.