URetail: Privacy User Interfaces for Intelligent Retail Stores

Frederic Raber, Nils Vossebein

URetail: Privacy User Interfaces for Intelligent Retail Stores

Frederic Raber and Nils Vossebein

DFKI, Saarland Informatics Campus
frederic.raber@dfki.de, Nils.Vossebein@gmx.de

Abstract. Amazon recently opened its first intelligent retail store, which captures shopper movements, picked-up products and much more sensitive data. In this paper we present a privacy UI, called *URetail*, that returns to the customer control over his own data, by offering an interface to select which of his private data items should be disclosed. We use a radar metaphor to arrange the permissions with ascending sensitivity into different clusters, and introduce a new multi-dimensional form of a radar interface called the privacy pyramid. We conducted an expert interview and a pilot study to determine which types of data are recorded in an intelligent retail store, and grouped them with ascending sensitivity into clusters. A preliminary evaluation study shows that radar interfaces have their own strengths and weaknesses compared to a conventional UI.

1 Introduction

Retail stores like Amazon Go collect a massive amount of deanonymized private data on each of their customers in order to offer their services. Amazon uses "sensor fusion" to follow the customer from the entrance gate throughout the shop, registering products being picked up, placed back and/or viewed, stopping points and most likely also the exact route throughout the store. Although the Amazon Go service saves time and is very convenient, not all shoppers are happy with the new store concept: The whereabouts of the data and what else it is used for remain as unclear as the description of technologies used and what data is recorded by them.

2 Related work

There is plenty of work regarding data privacy in social networks [6,9], location sharing [5] and mobile app permission setting [7], but so far, to the best of our knowledge, nobody has explored how these interfaces work for retail data, or how they could be improved. Privacy setting interfaces are mostly realized as list-based interfaces, as for example on Facebook: All data types (photos, videos, comments etc.) are listed one after the other, with a button or slider next to each item, to switch the privacy policy to disclose/undisclose for that type of data. Although such interfaces can be efficient for the setting task alone, it is

hard to have a clear overview on the current state of the settings as a whole, and which settings might be unusual and need some tuning [1]. Furthermore, it is obvious that they are not perceived as attractive and fun to use: Research in the past has shown that tuning the privacy settings is mostly perceived as a burdensome and boring task [3,8], which leads users to almost never adjust the standard settings, resulting in suboptimal privacy settings.

A different UI concept that is used in research is the *radar metaphor*: The different data items are first clustered into different groups of data types. In the second step, the items of each cluster are sorted by ascending privacy rating, for example. Christin et al. provided such an interface, called a *privacy radar* [1], to visualize the privacy threats in participatory sensing applications. Their evaluation showed that the radar interface provided a clearer overview on the privacy threats, and significnatly raised user awareness and interest in adjusting privacy settings. The radar metaphor is also highly appropriate [2] for space-constrained devices like smartphones. The concept has also been used to select post recipients in social networks: Privacy Wedges [9] aligns the friends of a Facebook user, clustered into friend groups and ordered by ascending tie strength.

In this paper we want to examine whether a radar metaphor can be applied to the domain of intelligent retail data. We did some background research to investigate what data is typically collected inside an intelligent retail store, and checked whether the typical constraints of a radar interface (clustering data and sorting the clusters) can be met. We implemented a prototype of both a conventional list-based and extended radar interface, that allows the simultaneous view of several radar layers at once in a three-dimensional privacy pyramid. We compared the performance and user experience of both approaches in a preliminary evaluation.

3 Background research

We interviewed an employee of the Innovative Retail Laboratory [10], an intelligent retail store concept similar to Amazon Go, regarding the data that is gathered inside an intelligent retail store, to create a list of privacy-sensitive data, later called *permissions* or *items*. We went through the assistance systems of the IRL and the Amazon Go store, and collected data that is recorded to make the services work. In addition to the services and data types, we also recorded the stakeholders that are interested in this type of data or that offer the service. In a second step, we asked five participants (employees of our university) to cluster and sort the data types.

Table 1 contains a list of observed private retail data items together with the service where the data is used and the interested stakeholders. The participants produced a similar order for all clusters, except for the *personal data* cluster. This cluster was therefore realized as a list in URetail. The items in the other clusters are sorted with ascending privacy rating in the table.

		Services	Stakeholders
Personal Data	*Address* *Birthday* *Name* *Gender*	Invisible checkout	Retailer, friends, family
	Income	Product recommender	Retailers, 3rd parties
Location data	*Recent visits:* *- Province* *- City* *- Address*	Invisible checkout	Retailer, friends, family
	Movement	Customer heatmap	Retailer
Shopping Receipt	*Loyalty points* *Items bought:* *- Amount* *- Category* *- Price*	Invisible checkout	Retailer, friends, family
Interests	*Wishlist*	Digital shopping list	Retailer, friends, family
	Recently viewed	Product recommender	Retailers, 3rd parties

Table 1. Data recorded in an intelligent retail store and services where it is used, assigned to groups and sorted with ascending sensitivity.

4 URetail: a radar interface for intelligent retail store data

Inside URetail, the data clusters are visualized by wedges in the radar; the layers inside each wedge represent the different data types, ordered in ascending sensitivity from the center to the rim. To set the disclosure settings for a data group, the user clicks on a wedge layer or drags from the center of the radar to a wedge layer (1). All data types inside the group from the lowest sensitivity (center) up to the selected layer are then set to disclose. If the severity order is not correct, the user can modify the order by drag & drop in the list view beneath each wedge (2). Alternatively, to adjust the disclosure settings using the radar interface, the user can also disclose/undisclose a data type by clicking on the data items inside the list view (2). The four different *stakeholders* are again realized by four different webpages, accessible by a navigation bar on the left-hand side just like in the list interface.

The radar interface also supports an overview of the settings of all stakeholders at a glance, using a 3D pyramid below the wedges of the radar (3), later called the *privacy pyramid*. The pyramid consists of four different layers, representing the four different *stakeholders*. Each layer has four edges, representing the four different *data groups*. The more data is disclosed inside a data group, the larger is the corresponding edge in the pyramid. To get an impression of where the settings are unusual and probably misconfigured, it is possible to display the privacy pyramid of an average user as a transparent overlay.

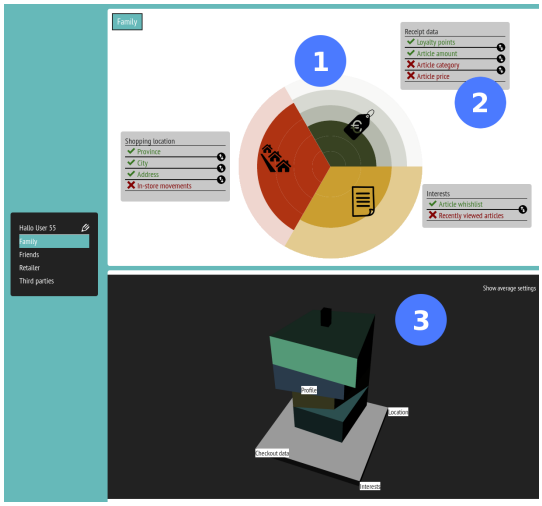

Fig. 1. Radar interface: Data types are arranged in groups, sorted by sensitivity.

5 Evaluation and discussion

For evaluation purposes, we implemented a list-based interface, as described in the "Work done so far" section, and let 21 participants (students and university employees) test both interfaces on a desktop PC, followed by an interview where they also had to rate on a scale from 1 (best) to 5 (worst) which interface was better to spot *whether* there are differences from an average privacy profile, *where* they are and how an average profile looks, followed by the attrakdiff [4] usability questionnaire. The participants stated that they first had to get used to the radar interface, but after a short trial phase, it felt faster to use, which is also reflected in a higher pragmatic score in attrakdiff ($M_{radar} = 1.99$, $M_{list} = 0.69$, $Z = -3.785$, $p < 0.001$). The privacy pyramid makes it easier to spot *whether* there are differences ($M_{radar} = 1.62$, $M_{list} = 2.14$, $T = 2.75$, $p = 0.012$), whereas it easier to see *which* items are different ($M_{radar} = 2.19$, $M_{list} = 1.67$, $T = 2.95$, $p = 0.008$) and *how an average setting* looks ($M_{radar} = 2.62$, $M_{list} = 1.81$, $T = 3.07$, $p = 0.012$) with the list-based UI. According to the attrakdiff results, the radar interface had a significantly better user experience and was more fun to use ($M_{radar} = -0.745, M_{list} = 2.28, Z = -4.02, p < 0.001$). To conclude, both radar and list interface have their own strengths and would have to be combined to achieve an optimal performance. The radar is perceived as more interesting and fun to use, which allows better motivation of users to do the boring task of privacy setting. Furthermore, it is perceived as faster after a training phase. In future work, we would like to conduct a lab study to explore whether the concept is applicable for mobile devices, how both interfaces can be combined and how the time needed for interaction changes over time, once the subjects get used to the interface.

References

1. Christin, D., Michalak, M., Hollick, M.: Raising user awareness about privacy threats in participatory sensing applications through graphical warnings. In: Proceedings of International Conference on Advances in Mobile Computing #38; Multimedia. pp. 445:445–445:454. MoMM '13, ACM, New York, NY, USA (2013), http://doi.acm.org/10.1145/2536853.2536861
2. Christin, D., Reinhardt, A., Hollick, M., Trumpold, K.: Exploring user preferences for privacy interfaces in mobile sensing applications. In: Proceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia. pp. 14:1–14:10. MUM '12, ACM, New York, NY, USA (2012), http://doi.acm.org/10.1145/2406367.2406385
3. Ghazinour, K., Matwin, S., Sokolova, M.: Monitoring and recommending privacy settings in social networks. In: Proceedings of the Joint EDBT/ICDT 2013 Workshops. pp. 164–168. EDBT '13, ACM, New York, NY, USA (2013), http://doi.acm.org/10.1145/2457317.2457344
4. Hassenzahl, M., Burmester, M., Koller, F.: Attrakdiff: Ein fragebogen zur messung wahrgenommener hedonischer und pragmatischer qualitaet. In: Szwillus, G., Ziegler, J. (eds.) Mensch & Computer 2003: Interaktion in Bewegung. pp. 187–196. B. G. Teubner, Stuttgart (2003)
5. Jedrzejczyk, L., Price, B.A., Bandara, A., Nuseibeh, B.: "privacy-shake",: A haptic interface for managing privacy settings in mobile location sharing applications. In: Proceedings of the 12th International Conference on Human Computer Interaction with Mobile Devices and Services. pp. 411–412. MobileHCI '10, ACM, New York, NY, USA (2010), http://doi.acm.org/10.1145/1851600.1851690
6. Kauer, M., Franz, B., Pfeiffer, T., Heine, M., Christin, D.: Improving privacy settings for facebook by using interpersonal distance as criterion. In: CHI '13 Extended Abstracts on Human Factors in Computing Systems. pp. 793–798. New York, NY, USA (2013), http://tuprints.ulb.tu-darmstadt.de/3490/
7. Lin, J., Liu, B., Sadeh, N., Hong, J.I.: Modeling users' mobile app privacy preferences: Restoring usability in a sea of permission settings. In: Symposium On Usable Privacy and Security (SOUPS 2014). pp. 199–212. USENIX Association, Menlo Park, CA (Jul 2014), https://www.usenix.org/conference/soups2014/proceedings/presentation/lin
8. Majeski, M., Johnson, M., Bellovin, S.M.: The Failure of Online Social Network Privacy Settings. Tech. Rep. CUCS-010-11, Department of Computer Science, Columbia University (Feb 2011)
9. Raber, F., Luca, A.D., Graus, M.: Privacy wedges: Area-based audience selection for social network posts. In: Twelfth Symposium on Usable Privacy and Security (SOUPS 2016). USENIX Association, Denver, CO (2016), https://www.usenix.org/conference/soups2016/workshop-program/wpi/presentation/raber
10. Spassova, L., Schoening, J., Kahl, G., Krueger, A.: Innovative retail laboratory. In: Roots for the Future of Ambient Intelligence. European Conference on Ambient Intelligence (AmI-09), 3rd, November 18-21, Salzburg, Austria. o.A. (2009), https://www.dfki.de/web/forschung/publikationen/renameFileForDownload?filename=AmI-Landscape-InnovativeRetailLab.pdf&file_id=uploads_338