Privacy concerns arising from internet service personalization filters

Ansgar Koene, Elvira Perez, Christopher J. Carter, Ramona Statache, Svenja Adolphs, Claire O'Malley, Tom Rodden, and Derek McAuley
HORIZON Digital Economy Research, University of Nottingham, United Kingdom
University of Nottingham Innovation Park, Triumph Road
Nottingham, NG7 2TU, UK
+44 0115 8232551
{ansgar.koene, elvira.perez, christopher.carter, ramona.statache, svenja.adolphs, claire.omalley, tom.rodden, derek.mcauley}@nottingham.ac.uk

ABSTRACT

Personal service customization, or personalization, is one of the core tools that are being used by on-line providers of information services such as search engines, social media, news sites and product recommender systems to optimize the individual user experience in hopes of attracting and keeping users. In this paper we will examine the user profile models that are used to achieve this information personalization. From a citizen centric perspective, our concerns focus on the degree of privacy intrusion that is implicitly required to determine the parameter settings of the information filter profile and the ethical implications of the personal behavior predicting properties of the user model itself.

Categories and Subject Descriptors

K.4.1 [**COMPUTERS AND SOCIETY**]: Public Policy Issues – *Ethics, Privacy, Use/abuse of power.*

General Terms

Algorithms, Measurement, Performance, Design, Economics, Reliability, Security, Human Factors, Theory, Legal Aspects

Keywords

Personalization; Behavior profiles; Information filtering; position paper.

1. INTRODUCTION

The massive growth of digital data creation, with more than 90% created in the last couple of years, a 400% data collection increase year-over-year in 2012 [1] and almost 1 billion active and indexed websites [2] has made sifting through and ranking of information into the primary challenge for many internet uses. The basic concept behind personalization of on-line information services is to shield users from the risk of information overload, by pre-filtering search results based on a model of the user's preferences. As such, the motivation behind these systems is ethically sound. The user profile model that is used to predict a user's preferences, however, and the methods by which the data is acquired for tuning it, do raise concerns.

The user profile model, is often derived from past online behavior of the user [3], which is logged with the user account. This data is primarily derived from previous visits to the service providing site, but in some cases may also involve the use of 'tracking cookies' to gather information about the user's behavior on other websites in order to further fine tune the user profile [4]. Other frequently used sources of data for tuning the user profile models include data concerning the behavior and preferences of people within the social network of the user [5]. Leaving aside the obvious ethical concerns relating to the use of 'tracking cookies', tracking of user activity on the service site itself can also produce highly detailed personality profiles, especially when the service provider is a search engine or social media site that is heavily accessed by the user and provides a wide diversity of services. In essence, the process of creating a user profile for the service personalization involves exactly the kinds of privacy invasive data mining that we have previously argued to require strictly maintained informed consent procedures to maintain proper research ethics when employing such data mining for academic research [6,7]. It is therefore ethically highly problematic that the need to maintain an advantage over competing services frequently results in service providers choosing not to inform their users about the personalization methods that are being used. Despite these ethical issues concerning the data that is used for creating the user profile models, the main concern we would like to draw attention to in this paper is not the 'raw data' but rather the user profile itself.

The user profile model is in essence an operationalization of the data mining efforts, built to anticipate the user's behavior, interests and desires. A perfect user model would ideally, from the service provider's perspective, enable the service provider to perfectly predict the decision a user would make for any given choice. If successful, this would in effect produce a Pandora's box of potential privacy violations, just waiting to happen. To find a user's weaknesses, for instance, it would suffice to query the user's profile model with a range of choices and observe the predicted responses. Such an idealized perfect user profile model is of course not (yet) possible, and would require access to data that is not (yet) in the on-line domain. Increased prevalence of internet connected sensors, i.e. Internet of Things, however may change this in the near future.

In section 2 we provide a brief review of information personalization systems and the role of user profile models in these. Section 3 describes the process of data collection for generating person profiles. Section 4 conceptually summarizes the frequently used method of constructing the user profile model from the collected data. Section 5 discusses some of main uses and possible abuses for which the personalization profiles could be used.

2. Brief review of personalization systems

Ranking and/or filtering of Internet search results and Social Media-/News-feeds for increased user satisfaction is in essence the same challenge as that is posed to recommender systems used by the likes of Amazon.com, YouTube, Netflix, TripAdvisor, etc. to suggest items the user might be interested in. Recommender systems emerged as an independent research area in the mid-1990s. These first recommender systems [8] applied collaborative-filtering which matches users who have in the past made similar choices (i.e. given similar ratings, or 'clicked' on similar items) on the assumption that they have similar preferences and will therefore be interested in recommendations for items that these users rated highly. Modern recommender systems use (combinations of) various types of knowledge and data about users and previous transactions stored in customized databases. The knowledge and data about the users is collected through explicit ratings by the users for products (e.g. purchase feedback on Amazon), inferred by interpreting online actions of users (e.g. navigating to a particular product), through monitoring of social networks and social media activity (e.g. Facebook Social Graph) and increasingly through data from personal networked devices (e.g. Mobile phone location data).

The three main classes of recommender systems are:

1. Content-based, where the system recommends items based on their similarity to items the user expressed interest in, e.g. purchased, clicked on, searched for etc., in the past. The similarity of items is calculated based on the features associated with the compared items.
2. Collaborative-filtering, users are given recommendations for items that other users with similar tastes liked in the past. The similarity in taste of two users is calculated based on the similarity in the rating histories of the users.
3. Community-based, where the system recommends items based on the preferences of the user's friends. This is similar to collaborative filtering except that the selection of peers that are used for selecting the recommendations is based on an explicit 'friendship' link instead of being deduced from patterns of similar past behavior. Such 'social recommender' systems are poplar in social-network sites [9].

In practice many recommender systems are hybrid systems that try to balance the advantages and disadvantages of each class [10]. Collaborative and community based systems, for instance, suffer from an inability to recommend items that have not yet been rated by any of the potential peers of the user. This limitation however does not affect content-based system as long as the new item is supplied with a description of its features, allowing it to be compared to other items that the user has interacted with in the past.

A comprehensive introduction to recommender systems is provided in [11].

3. User profiles information gathering

We will now give an overview of common user profile data collection methods, including discussions regarding the impact on privacy, the growing role of social networks and issues related to trading of data with third-parties. Most of the examples in this section will refer to Google, simply because of its dominant position in information services. Reference to Google's practices is not meant to imply that their practices are any more or less ethically acceptable than any other service.

3.1 Data collection

Data collection about users typically uses a range of different channels. At the most basic level the service provider, e.g. Google, records the immediate interaction of the user with its service, e.g. the search and browsing activity. With respect to this type of data collection, the Terms of Service [12] and accompanying Privacy Policy [13] which Google presents when a new account is created state that:

"When you use our services or view content provided by Google, we automatically collect and store certain **information in server logs**. This includes:

- details of how you used our service, such as your search queries.
- telephony log information, such as your phone number, calling-party number, forwarding numbers, time and date of calls, duration of calls, SMS routing information and types of calls.
- Internet protocol address.
- device event information, such as crashes, system activity, hardware settings, browser type, browser language, the date and time of your request and referral URL.
- cookies that may uniquely identify your browser or your Google Account."

For the most part the information that is collected through the server logs is unsurprising. Probably least obvious amongst this list are the collection of the phone related information, the system activity and hardware settings. It should be noted however that none of this information actually requires that the user has an account with the service provider (Google). Based on the IP address, phone information or other hardware information, logs of search queries that are performed while the user is not logged in to an account could in principle still be linked to the profile associated with the user's account.

For the construction of a behavior profile, tracking of search queries (or more generally the way in which the primary service function is used) remains a core defining element since this is what the personalization must aim to improve to satisfy the user.

Other obvious data that is collected includes the information which users are asked to provide when they sign up to an account. This typically includes: a name, email address, telephone number and possibly even a credit card. Increasingly, thanks to improved face recognition algorithms, users are also strongly suggested to include a photo. Providing of fake inputs for this personal information is often the first action people take when they become more privacy sensitive. In itself this information is not particularly useful for the creation of a user behavior profile, but it does provide important linking information for associating user data that is gathered from different, nominally independent services.

More interesting and less obvious data which is mentioned in Google's 'Information that we collect' section in the Privacy Policy includes:

“We collect information [when you] visit a website that uses our advertising services or view and interact with our ads and content. This information includes:

- **Device information,** such as the hardware model, operating system version, unique device identifiers, and mobile network information including phone number.
- **Log information,** [as described earlier under 'server logs'].
- **Location information,** [determined] using various technologies, including IP address, GPS and other sensors that may, for example, provide Google with information on nearby devices, Wi-Fi access points and mobile towers.“

Often it is not clear to the user which service is providing the ads on a website, nor does the user know what ads to expect on a website before visiting it. The user therefore has no means of controlling which ad-providing service will know about their visit to a particular site. The only way for the user to regain agency and control over consent is to install ad-block software and/or disable cookies, both of which might disable some browser functionality the user may have been interested in.

The methods that are used for collecting data about web-browsing behavior rely on “various technologies to collect and store information [which] may include using cookies or similar technologies [e.g. pixel tags/Web beacons] to identify your browser or device when it visits a webpage.” … “We also combine this data among our services and across your devices for these purposes, for example, using information from your use of Search and your Gmail to show you personalized ads.”

From a user perspective unfortunately these 'various technologies' appear to all be beyond the control of the user and are mostly hidden so that the user frequently does not know that such data collection is taking place. This makes it very difficult for users to manage the level of information they wish to expose about themselves.

3.2 The role of Social Networks

Social Networks, like Facebook and Google+ play an increasingly important role in user profiling due to the richness of personal data they contain. In many ways a user's Facebook or Google+ page is nothing else than an elaborate exercise in self-profiling contained in a tightly templated structure that facilitates automated data extraction. To further enhance the depth of the user profile information on Social Network Sites (SNSs), users are repeatedly prompted to fill in more background details (e.g. “what was your role when you worked at X), 'tag' more photos and tell their 'friends' about the latest things they are interested in, while the profiling engine listens to their communications. Most important however is the 'friends' network, i.e. the 'Social Graph', itself which directly establishes the network of peers to use for Community-based recommending systems.

In the context of privacy/consent related issues, one of the main concerns with Social Network Sites is the loss of personal control over the information that is provided to the system, due to the bi-directional nature of the network. This was most prominently discussed in relation to image tagging [14] where users can tag other people, revealing their presence at an event without the explicit consent of that person. The same holds true, however, for many other activities on social networks, including the sending of 'friend' requests. Even if the request is declined, it reveals something about both sides of the interaction. This is especially true since it is notoriously difficult to truly delete something from social network sites, where 'removing' usually only means hiding it from other normal Social Network Site users [15]. Further more, it is not at all clear if/how the parameters on the user profile model are updated when data is 'removed' from the social network.

3.3 Trade in personal databases

Since trading of personally identifiable data to third-parties, without the explicit consent of the individual to whom the data refers, is generally considered to be a too severe privacy violation that would have repercussions for the parties doing the trade, such data is commonly not traded. Instead the policy regarding 'Information we share' [13] states that:

“We do not share personal information with companies, organisations and individuals outside of Google unless one of the following circumstances applies:

With your consent

We will share personal information with companies, organisations or individuals outside Google when we have your consent to do so. We require opt-in consent for the sharing of any sensitive personal information. [Such an opt-in may however be included in the Terms and Conditions that users commonly click-sign without reading when they install new apps.]

For external processing

We provide personal information to our affiliates or other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures.

For legal reasons

We will share personal information with companies, organisations or individuals outside Google if we have a belief in good faith that access, use, preservation or disclosure of the information is reasonably necessary [for law enforcement].”

However in the second to last paragraph they also state that:

“We may share aggregated, non-personally identifiable information publicly and with our partners – like publishers, advertisers or connected sites. For example, we may share information publicly to show trends about the general use of our services.“

Since the data that is shared with partner organizations is aggregated and non-personally identifiable (we will assume that this is indeed the case, unlike [16]) it can not contribute very specific data points to the user profiles. It does still hold a lot of value for the tuning of user profiles, however, since data of the type: 'N percent of people with characteristics J and K chose option A'; does help to shape the predicted behaviour probability distributions for 'people with characteristics J and K'.

4. Combining data into profile models

User profiles are most frequently represented by mapping the data in a high dimensional space [17, 18], with vectors denoting the past preferences the user expressed in their observed online behavior. In order to better capture the context dependent nature of human preference, especially in social settings, some personalization systems use context-aware generative models to adjust the multi-dimensional mapping according to context [19, 20, 21, 22]. Based on this multi-dimensional vector representation of the personal data profile, recommendations can then be generated by projecting the set of potential results into the same space and selecting those items that have the shortest distance from the personal data vectors.

When constructing the personal profile model there are a number of choices that needs to be made, foremost among which is the question of how to define the dimensions. What kind of online items, behavior and communications should be classified as being aligned along a single dimension? What should the unit scales be on each dimension? e.g. is the difference between red and green colors more significant than a doubling in size of an object? In some cases the task might literally consist of comparing apples with oranges, the answer to which is obviously context dependent. The quest to solve these dilemmas is one of the reasons why tech companies like Google and Facebook are investing heavily in 'strong AI' research.

Aside from the ethical issues related to the acquisition of input data for the creation of the model, which we discussed in section 3, the user profile model itself also raises some interesting ethical issues. The purpose of the model is to predict a person's preferences, which is done by a process of nearest-neighbor matching in the mapped multi-dimensional space. Any additional information that is inferred from the accumulated input data therefore only exists implicitly as long as no specific search is done. Does the implicit nature of the information automatically shield the model from any claim of privacy invasion, no matter how personal or intimate the inferred knowledge about a person is?

5. Uses and possible abuses

The primary uses and purpose of user profile models are to facilitate personalization of the information service (Search, News-feed, product recommendation, etc.) to improve the user experience, as well as facilitating targeted advertising to improve click-through and sales rates.

Since the user profile model is in essence an attempt at profiling and anticipating a user's preferences and behavior, one could easily imagine using/abusing the model for any situation that involves personality profiling. If the user profile models were sufficiently reliable, recruitment agencies could simply arrange submit targeted questions to the profile models to identify the most suitable candidates for jobs possible making job interview redundant. Law enforcement agencies might use the user profile models to narrow the field of suspects or use the profile model to predict the actions of a specific suspect. Teachers might submit queries to the profile models of pupils to help them find the most engaging way to present their course material. Viewed from a techno-utopian perspective, the list of beneficial uses appears endless. Viewed from the citizen-user perspective who's personal profile is being analyzed, however, each of these use cases is ethically highly contentious and would require a lot of safeguards to protect citizens from abuse. None of the examples we listed are currently feasible, due to the low fidelity of the model predictions at this time. The use of the user profiles for targeted advertising, however, has already revealed some of the potential pitfalls as shown by the case in 2012 when the Target used this type of data mining to identify and inadvertently reveal a girl's pregnancy to her father [23].

6. Internet of Things

One of the reasons why the user profile models still have only limited ability to anticipate user preferences is that the data they are build on is mostly confined to the behaviors people exhibit online. In order to get a more complete profile of a person it will be vital to incorporate data from real-world behavior. The first move in that direction was obviously location tracking in smart phones which could for instance help to disambiguate location dependent context effects on user preferences. Fitness monitors and health trackers (e.g. Apple Health-Kit) are now set to add information about the physiological state of the user.

The main ethical concern that is raised by the introduction of Internet of Things devices as additional data source for the user profiles is the inherent privacy invasiveness of the increasingly pervasive monitoring.

7. Conclusion

To summarize, both the data acquisition and data mining that are used to tune personalization profiles for information filtering and the user profile models themselves are ethically contentious practices. In order to counter balance the potential privacy invasiveness of these practices they should require a high level of transparency and clearly informed consent from the service users. It is therefore all the more problematic that many users are not, or only vaguely, aware of the fact that major services, e.g. Google search and Facebook Newsfeed, employ personalized information filtering.

8. ACKNOWLEDGMENTS

This work forms part of the CaSMa project supported by ESRC grant ES/M00161X/1. For more information about the CaSMa project, see http://casma.wp.horizon.ac.uk/ .

9. REFERENCES

[1] GovLab, 2013. The GovLab Index: The Data Universe. *GovLab Blog*, (August 22, 2013), NYU Polytechnic School of Engineering. http://thegovlab.org/govlab-index-the-digital-universe/

[2] Internet live stats, 2015. Total Number of Websites. *Internet live stats*. http://www.internetlivestats.com/total-number-of-websites/

[3] Speretta, M., Gauch, S., 2005. Personalized search based on user search histories. *Web Intelligence, 2005. Proceedings. The 2005 IEEE/WIC/ACM International Conference on*, vol., no., pp.622,628, 19-22 Sept. 2005. doi: 10.1109/WI.2005.114

[4] Rohle, T., 2007. Desperately seeking the consumer: Personalized search engines and the commercial exploitation of user data. *First Monday*, [S.l.], sep. 2007. ISSN 13960466. http://journals.uic.edu/ojs/index.php/fm/article/view/2008/1883.

[5] Ma, H., Zhou, D., Liu, C., Lyu, M.R., King, I., 2011. Recommeder systems with social regularization, *WSDM '11 Proceedings of the fourth ACM international conference on*

Web search and data mining, pp287-296. 2011. doi: 10.1145/1935826.1935877

[6] Koene, A., Perez, E., Carter, C.J., Statache, R., Adolphs, S., O'Malley, C., Rodden, T. and McAuley, D., 2015. Research Ethics and Public Trust, Preconditions for Continued Growth of Internet Mediated Research, *1st International Conference on Information System Security and Privacy (ICISSP)*, Angers, France, February 9-11, 2015.

[7] Koene, A., Adolphs, S., Perez, E., Carter, C.J., Statache, R., O'Malley, C., Rodden, T. and McAuley, D., 2015. Ethics considerations for Corpus Linguistics studies using internet resources, *Corpus Linguistics 2015*, Lancaster, UK, 21-24 July, 2015.

[8] D. Goldberg, D. Nichols, B.M. Oki, D. Terry, 1992. Using collaborative filtering to weave information tapestry, *Commun. ACM*, 35(12), 61–70.

[9] J. Golbeck, 2006. Generating predictive movie recommendations from trust in social networks, *Trust Management, Proceedings 4th International Conference, iTrust 2006*, Pisa, Italy, 93–104, May 16-19, 2006.

[10] R. Burke, 2007. Hybrid web recommender systems, *The AdaptiveWeb*, 377–408. Springer Berlin / Heidelberg.

[11] L. Rokach, B. Shapira, and P.B. Kantor. 2011. *Recommender systems handbook*. Vol. 1. New York: Springer.

[12] Google Terms of Service, https://www.google.co.uk/intl/en/policies/terms/

[13] Google Privacy Policy, http://www.google.com/policies/privacy/

[14] A. Besmer, H. R. Lipford. 2010. Moving Beyond Untagging: Photo Privacy in a Tagged World. *CHI 2012: Privacy*, pages 1563- 1572

[15] Z. Whittaker. 2010. Facebook does not erase user-deleted content." *ZDNet, April* (2010). http://www.zdnet.com/article/facebook-does-not-erase-user-deleted-content/

[16] Netflix official blog announcement, March 12, 2010. http://blog.netflix.com/2010/03/this-is-neil-hunt-chief-product-officer.html

[17] F. Abel, Q. Gao, G.-J. Houben, and K. Tao. 2011. Analyzing user modeling on twitter for personalized news recommendations. *In User Modeling, Adaption and Personalization*, pages 1–12. Springer, 2011.

[18] N. Matthijs and F. Radlinski. 2011. Personalizing web search using long term browsing history. *In WSDM 2011*, pages 25–34.

[19] Z. Zhao, Z. Cheng, L. Hong, E.H. Chi. 2015. Improving User Topic Interest Profiles by Behavior Factorization. *In WWW 2015,* pages 1406-1416.

[20] M. Qiu, F. Zhu, and J. Jiang. 2013. It is not just what we say, but how we say them: LDA-based behavior-topic model. *In SDM*, pages 794–802.

[21] J. Tang, M. Zhang, and Q. Mei. 2013. One theme in all views: modeling consensus topics in multiple contexts. *In SIGKDD 2013*, pages 5–13.

[22] H. Yin, B. Cui, L. Chen, Z. Hu, and Z. Huang. 2014. A temporal context-aware model for user behavior modeling in social media systems. *In SIGMOD 2014*, pages 1543–1554.

[23] K. Hill. 2012. How Target Figures Out A Teen Girl Was Pregnant Before Her Father Did. Forbes 2/16/2012. http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/

Columns on Last Page Should Be Made As Close As Possible to Equal Length