# Review on "The best privacy defense is a good privacy offense: obfuscating a search engine user's profile"

**Joshua Fenech** *, **and Omar Elsabrout** *

*Jean Monnet University

Submitted to the faculty of science and technology at Jean Monnet University

**Since the growth rate of the Internet is almost exponential, it has a drastic effect on people's lives everyday. Such effect is accompanied with many issues such as user privacy. It is not settled until now how service providers are allowed to use stored information of the users and compromise their privacy. Jörg Wicker and Stefan Kramer introduce a tool that utilizes machine learning and data mining to confuse search engines to protect the user's privacy by obfuscating exploited personal information. Not only methods are introduced for such technique, but also an experiment to evaluate its results indicating whether this approach should be investigated further.**

## Introduction

The motivation behind providing this approach is that the current privacy protection have major flaws. On one hand, users rely on service providers to process their data, on the other hand, providers do not have any advantage in user privacy preserving technologies as the analysis of this data and sharing it with advertisers is the basis of their business model. No doubt that providers such as search engines must store information on users. Nevertheless, these data can be used to generate detailed profiles on a large scale and identify unidentified users. As mentioned, Jörg Wicker and Stefan Kramer target privacy from another perspective. Hence, they suggest a user tools to defend her or his privacy so the user does not have to rely on the other uncontrollable side for this issue. Data is conventionally stored in large scales and analyzed automatically using data mining technologies. As a result, the intuitive approach to protect the users private information would be to flood the data storage with random data and hope the users interest or identity would be obfuscated. On the contrary, data mining algorithms are designed to distinguish a signal from random noise. Consequently, this approach will fail in most settings where the data is analyzed with sophisticated data mining algorithms. The paper tackles this issue in a more highly developed manner as it gives a brief discussion of the user and search engine model in addition to the proposed method. Moreover, it shows the details of the experimental set-up and results. Taking into account, the paper should be considered as proof-of-concept and not a final product ready for the market. In this review, we present pointers for the given approach and criticize it by explaining its strong arguments and also its weak ones. This is not meant to be a summary of the tackled paper as we merely mention concepts and do not dive into details.[1].

## Discussion

One of the first obstacles that is faced and discussed in the paper, is the user model. The authors admit a problem of major simplification for the user's interest categories as a result of reducing these categories to one at a time. The reason behind such simplification is to simplify the evaluation so they can compare the reaction of the search engine to one interest category. Although they stated that future work will address users with multiple interest categories and users with variably strong interest in multiple categories, we think that such simplification needs to be accompanied with assurances of the ability to upscale the model for multiple categories or at lease some pointers for such ability. These assurances are not provided which leaves the problem unattended. Nonetheless, another simplification is justified which is to only address query results that provided ads due to the problem's nature.

Another obstacle that might be rather unavoidable is that obfuscating a search engine user's profile, even though if it protects the user's privacy, reduces the user's experience quality. A user who utilizes this approach will lose most of personalized services and automated customizations provided by search engines if not all of them. We know that this is a decision that users must make. However, it is a hard one as these services are more practical and useful so the trade-off might not be fair. The author's assumption that user prefers privacy overlooks the idea that the number of those users can be low in comparison with the ones who prefer personalization. Despite that, we think that it is still perfect to execute the obfuscation idea in form of a tool that can be easily deactivated if the user wanted. This does not affect the user's profile if he or she wishes to return to using the search engines normally.

In addition, obfuscating search engines and service providers waste their resources and invalidates their research results and statistical studies that might lead to new applications based on the user's needs. These needs are usually investigated by online surveys and mining user data which will be useless because of mining fake or randomized data.

## Method

Since the full knowledge of the states and information of the search engine are not available, the algorithm behaves according to only the feedback from the search engine in the form of ads. The method of such approach is to based on text ads, which is certainly a limitation as mass media now depends on many more forms of advertisement that involve audio and video. Nonetheless, it is considered a great start though and a milestone for promising future work. Service provider such as search engines display targeted ads depending on the submitted query by the user which must go through an interest cat-

**Reserved for Publication Footnotes**

egory process to categorize the query. In addition, displayed ads also depend on the user's profile. This plays a greater role specially for advertisers as dedicating ads to targeted audience is more efficient and promises perfecting the selling point.

For such process to succeed, ads must be processed and assigned to categories in advance to be displayed to their matching needs. Not only ads are assigned, but also users are assigned to categories depending on their profiles either by their user accounts or by artificial ones depending on IP tracking and cookies.

Revisiting the concept of privacy defense which is the main purpose of Jörg Wicker's and Stefan Kramer's method, privacy metrics and standards must be presented to evaluate such method. For instance, an objective function is presented in the paper for such purpose [**1**].

$$\sigma(\kappa_i, P) = \sum_{p_j \in P, \kappa_j \in T} p_j d_T(\kappa_i, \kappa_j) \qquad [1]$$

According to this notation, the user's interest category is expressed with $\kappa$ and these categories are predefined by the search engine. Moreover, $P$ represents the distribution of probabilities of the categories, $T$ represents the category tree and $d_T$ is the tree distance. This objective function is explained in details in the original paper. However, our report is not interested in such redundancy. Our interest resides in the significance of $\sigma$ which represents the score or the distance between the user's current interest category and the assigned category to the user. This $\sigma$ shows how the approach appears to be dynamic and it also shows the space margin of the algorithm to learn from the search engine's response to ad displaying.

The second component that is required for privacy defense is using the feedback of ads. This opens the discussion of category prediction of ads because search engines provide example queries for each category. These example queries or sample queries of category trees are the main input to train classifiers for ad categorization. Not only one classifier in this case, but as many classifiers as the number of available categories as every category has its own classifier. After certain training period, these classifiers can be used for more than classifying queries. Also, they can be used to classify any plain text which enables processing all text-based ads. As a result, prediction on ads works very well thanks to the similarities of structure between queries and text-based ads.

## Experiment and Results

Considering the environment of the presented experiment in the paper, we find that it was redundant to execute the experiment with submitting queries from random categories as it does not provide relevant results and does not contribute in the significance of the privacy offense method. On the contrary, submitting queries from the category that is the furthest away from the user's interest category is more relevant to the privacy offense method 1.

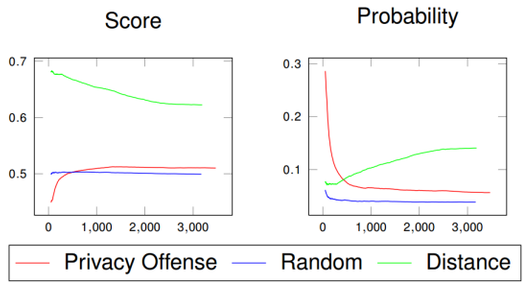


**Fig. 1.** Results

According to Wicker's experiment, all users submit random queries from their batch of interest categories in 10% of the cases. These outputs are based on using twenty categories in the experiment environment which we believe is sufficient in the context of an experiment. Upscaling the method would actually lead to more issues with greater number of users and interest categories. Despite that, it was fairly mentioned in the future work section that it is a major concern to continue working on the method and crucial to its development.

## Conclusion

To sum up, the experiment is successful to a certain extent with respect to the assumed limitations. Nevertheless, we still need further research and more elaborate experiment environments.

There are more areas that deserve studying and should be tackled during the development of such tool like the fact that models of search engines also rely on time and date of the query which is a factor that should be considered and taken advantage of. At the end of the day, the major simplification of learning for only one interest is still the major concern and the greatest limitation of the tool. Future work is interesting as it can involve more feedback than just ads from search engines but also use more features that they provide to predict their models and reactions. This could lead to a more sophisticated tool and could provide a better privacy defense model.

In this report, we discussed the main points of interest in the research paper while criticizing its weak and strong arguments. We started by the motivation behind the research in the introduction. Then, we presented how the discussion in the paper had strong arguments but with a few flaws. Afterwards, we discussed the method itself and how is it modeled which is the most important and interesting part of the paper. Last but not least, we mentioned how the results of the experiment and their environment contribute to the results and how they can improve.

**ACKNOWLEDGMENTS.** This work was part of an assignment for a research methodology course.

1. **Jörg Wicker and Stefan Kramer. The best privacy defense is a good privacy offense: obfuscating a search engine user's profile. Data Min. Knowl. Discov., 31(5):1419–1443, 2017.**