Visualizations to Teach about Mobile Online Privacy

Christine Mekhail, Leah Zhang-Kennedy, Sonia Chiasson

Carleton University, Ottawa Canada
{christinemekhail, leahzhang}@cmail.carleton.ca

Abstract. Users' privacy is increasingly being jeopardized by images uploaded using smartphones. These images have detailed metadata that can be used maliciously. We test the effectiveness of using visualizations to teach users how to protect themselves. Our preliminary results show that information presented visually was more effective and persuasive than text-only content.

1 Introduction

Many smartphones are shipped with location-based services enabled by default, potentially compromising user privacy. For example, location based data is automatically attached with every picture taken by most smartphone cameras; this process is known as *geo-tagging* [2]. Applications request sharing of location information at install time, leaving users with the impression that these settings cannot be changed. This information may be sold or stolen and used for online behavioural advertising or more malicious purposes such as identity theft and stalking [1, 3]. Users are increasingly uncomfortable with these privacy invasions. Recent surveys show that approximately half of users were completely opposed to their phone carriers storing their location [5] and were unwilling to share their location information in exchange for discounted mobile apps [4]. However, users continue to (unknowingly) share significantly more details online than they realize [2]. Seeing how users care about their own privacy, we argue that users are not given the proper knowledge to protect themselves against the issue of geo-tagging and the risks of online tracking.

Our aim was to raise users' awareness levels of the risks associated with geo-tagging and persuade users to act in a more privacy-aware manner. We designed infographics based on two distinct metaphors to teach users about these issues. We tested the effectiveness of two infographics (Figure 1) against a text-only condition. We also tested whether participants subsequently modified their geo-tagging and applications settings as an indicator of the persuasiveness of our materials.

2 Infographic Study

Our between-subjects study with 36 participants had an initial lab session where users completed a pre-test questionnaire, viewed the educational material, and completed a

Authors' copy. Published in adjunct proceedings of the International Conference on Persuasive Technology (PERSUASIVE) 2014, Cleup

post-test questionnaire. An online follow-up questionnaire was completed one week later to assess information retention and behavioural changes. Users were randomly assigned to the *Trail*, *Puzzle*, or text-only condition.

We have conducted preliminary analysis of users' Likert-scale responses, information retention, and open-ended comments. From Figure 1, we see that users initially had little knowledge of the related concepts, especially users in the infographic conditions. One week after viewing the materials, approximately two-thirds of users could accurately describe the concepts. We see a much larger increase in knowledge in the infographic conditions. We further see that users felt that the information was more useful when provided as an infographic. Perhaps more importantly, 64% of infographic participants reported taking additional actions to protect their mobile privacy such as disabling geo-location tracking; another 14% were already employing the recommended actions. For the text condition, 50% of users reported modified behaviour but many said that they would not have bothered learning the information on their own. Analysis is on-going and we will use the results of our analysis to inform the design of an online interactive comic meant to provide more in-depth learning and persuasion.

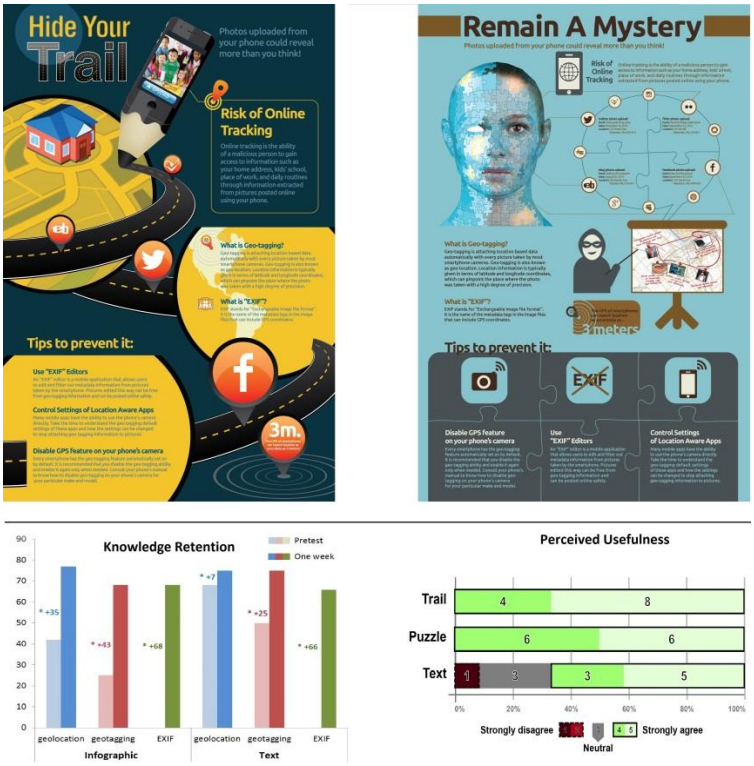

Fig. 1. Top: the *Trail* and *Puzzle* infographics. Bottom: preliminary results - pre/post-test knowledge of terms (left), usefulness of the information (right).

Acknowledgements

This project has been funded by the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the author(s) and do not necessarily reflect those of the OPC. Sonia Chiasson holds the Canada Research Chair in Human-Oriented Computer Security and acknowledges NSERC for funding the Chair.

References

1. Friedland, G., Maier, G., Sommer, R.,Weaver, N.: Sherlock holmes' evil twin: On the impact of global inference for online privacy. In: New Security Paradigms Workshop (NSPW) (2011)
2. Friedland, G., Sommer, R.: Cybercasing the joint: On the privacy implications of geotagging. In: USENIX Workshop on Hot Topics in Security (HotSec) (2010)
3. Goga, O., Lei, H., Parthasarathi, S.H.K., Friedland, G., Sommer, R., Teixeira, R.: Exploiting innocuous activity for correlating users across sites. In: International Conference on World Wide Web (WWW) (2013)
4. TRUSTe: Uk 2013 consumer data privacy study: mobile edition. http://www.truste.com/about-TRUSTe/press-room/news_uk_truste_customers_concerned_about_mobile_privacy (2013)
5. Urban, J., Hoofangle, C., Li, S.: Mobile phones and privacy. Public Law Research Paper (2012)