Privacy Trade-Offs of Geo-Location (Extended Abstract)

Laura Brandimarte
Eller College of Management – MIS
University of Arizona
lbrandimarte@email.arizona.edu

Alessandro Acquisti
H. John Heinz III College
Carnegie Mellon University
acquisti@email.arizona.edu

Pervasive computing and location-aware technologies are becoming an integral part of everyday life: satellite navigation systems have been available to the public since the year 2000, and smartphones are widespread, with approximately half of the adult population today owning one [1]. Soon enough, smart self-driving cars, not only aware of location, but also aware of other cars and systems nearby as well, may be just as common. Smartphone applications use location data in order to provide directions, reserve Lyft or Uber rides, communicate one's presence in a specific place on a social network, provide nearby restaurants recommendations, and so on. The benefits are as numerous and diverse as the smartphone apps that can be found on the market.

On the other hand, location-aware technologies raise privacy concerns for users, as they enable functionalities that may be perceived as intrusive. For example, such technologies allow companies to send "hyperlocal" targeted advertisements, which may not be well accepted by recipients. That is the reason why privacy-friendly solutions for such kind of targeting have recently been proposed [2]. Moreover, under certain conditions, a person's movements are enough to uniquely identify them. In fact, four (two) locations with associated timestamps are enough to identify on average 95% (50%) of cell-phone users, who can be located thanks to the signal their cell phones send to the respective carrier's antennas [3]. Such considerations may be especially disconcerting in cases where a specific location is of a sensitive nature in and of itself – e.g., a hospital specialized in a specific disease; a certain financial institution; a religious or political association; a neighborhood or a block that is often reported as a crime scene; a gentlemen's club.

This kind of sensitive situations are even more problematic because of the ease in sharing other people's locations, without the consent or knowledge of the parties at stake, for instance via social media [4]; or because of the widespread use of smartphone apps that "secretly" access one's location [5]. Methodologies have also been proposed to infer one's location simply from the content of non-geotagged messages posted on social media, or from the interactions with one's connections [6,7]. Sharing one's location seems to be hardly a choice anymore.

In this paper, we test for the effect of geo-location awareness on willingness to disclose personal, potentially sensitive information: Once we know that our location is identified, are we comfortable in disclosing further information about ourselves? Furthermore, the specific recipient of personal information affects the perceived sensitivity of such information and, therefore, willingness to disclose it: for instance, one may be willing to share one's location with family members, but not with an employer; or one may be comfortable sharing demographic information with Governmental institutions, but not location information. We therefore were also interested in the effect of the entity requesting information on perceived intrusiveness and willingness to disclose. Specifically, we tested whether Governmental institutions, which have recently been at the center of surveillance scandals in the US and abroad, are more or less trusted when it comes to collecting personal information, and investigated the role of surveillance primes in this scenario.

In a series of four experiments, we analyze individuals' reaction to geo-location (their location being identified), entity requesting the information, and surveillance primes in terms of perceived sensitivity of requested personal information and willingness to disclose it in an online questionnaire. In a first online experiment, we manipulate participants' awareness of their location being identified, and measure their willingness to reveal two types of personal information: engagement in unethical or somewhat compromising behaviors, and demographic information. In a second online experiment, we test for effects of institution requesting personal information. A third and fourth experiment measure the effect of institution and surveillance prime on perceived sensitivity (or

UEOP '16, 21 February 2016, San Diego, CA, USA
Copyright 2016 Internet Society, ISBN 1-891562-44-4
http://dx.doi.org/10.14722/ueop.2016.23001

intrusiveness) of requested information and actual propensity to disclose, respectively.

Overall, we find that awareness of being geo-located increases privacy concerns and has a negative impact on willingness to provide sensitive information, but no effect on disclosure of information that is perceived to be non-sensitive, such as demographic data. The inhibitory effect on the disclosure of sensitive information is more pronounced when the entity requesting it is not expected to, that is, when it is presented as a Governmental institution as compared to a research institution.

Acknowledgment

The authors would like to thank the National Science Foundation for supporting this research through grant NCRN-MN: Data Integration, Online Data Collection, and Privacy Protection for Census 2020, Award #1130706, (http://www.nsf.gov/awardsearch/showAward?AWD_ID=1130706).

References

[1] Economist, The (2015). Planet of the Phones. February 28. Available at: http://www.economist.com/news/leaders/21645180-smartphone-ubiquitous-addictive-and-transformative-planet-phones.

[2] Provost, F., Martens, D., & Murray, A. (2015). Finding Similar Mobile Consumers with a Privacy-Friendly Geosocial Design. *Information Systems Research, 26*(2), 243-265.

[3] de Montjoye, Y. A., Hidalgo, C. A., Verleysen, M., & Blondel, V. D. (2013). Unique in the Crowd: The privacy bounds of human mobility. Scientific reports, 3(1376), 1-5.

[4] Henne, B., Szongott, C., & Smith, M. (2013, April). SnapMe if you can: Privacy threats of other peoples' geo-tagged media and what we can do about it. In Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks, ACM, pp. 95-106.

[5] Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., Cranor, L., & Agarwal, Y. (2015). 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, ACM, pp. 787-796.

[6] Chandra, S., Khan, L., & Muhaya, F. B. (2011). Estimating twitter user location using social interactions – A content based approach. In Proceedings of the Third IEEE International Conference on Social Computing (SocialCom), IEEE, pp. 838-843.

[7] Cheng, Z., Caverlee, J., & Lee, K. (2010). You are where you tweet: A content-based approach to geo-locating twitter users. In Proceedings of the 19th ACM international conference on Information and knowledge management, ACM pp. 759-768.