JOURNAL OF SPATIAL INFORMATION SCIENCE
Number 19 (2019), p. 53 doi:10.5311/JOSIS.2019.19.608

EDITORIAL

Geospatial Privacy and Security

Location privacy has been a topic of research for many years but has recently experienced a resurgence in public interest. This renewed interest is driven by recent advances in location-enabled devices, sensors and context-aware technology, and the rise of the Internet of Things (IoT). The data generated via these sensors and devices is being collected, analyzed, and synthesized at an unprecedented rate. While much of this data is used in the advancement of products or services (e.g., navigation technologies), many individuals remain unaware of the information that is being collected, how it is being collected, and more importantly, how it is being used. The resulting information extracted from this personal data has contributed to significant advances in the computational and geospatial sciences, e.g., location recommendations or health services. However, these advances often come at the high cost of reduced location privacy.

From an academic perspective, geospatial privacy and security are crucial topics with roots in computer science, geography, sociology, and psychology, demonstrated by a long history of location privacy discussion in both industry and academia (c.f. [2, 3, 10, 1, 9]). While it is often discussed at a theoretical level, it has major societal implications that reach beyond these disciplines and into everyday life. To give a timely example, the U.S. government, acknowledging the potential for abuse, is limiting access to the data for the upcoming 2020 Census, choosing to protect citizen information via differential privacy [4] in order to impede the fusing of this data with other datasets for the purpose of identifying individuals [11].

In today's digital world, the "right to be forgotten" is becoming increasingly difficult to exercise. It is almost impossible to remove an individual's digital footprint from the public sphere. In a recent editorial in the New York Times, the CEO of the location data and intelligence company *Foursquare* called on the U.S. Congress to regulate the location industry [7]. The General Data Protection Regulation (GDPR) in Europe is a good first step, but the road is long. Citizens are beginning to take back ownership of their private information, asking corporations what they know about them, and requesting access to and removal of such data. There are regional variations in privacy regulations though, and the cost of violating an individual's digital privacy varies substantially. The plethora of services accessing your personal and location information is often hard to keep track of, meaning we often do not realize when our privacy has been violated.

Many aspects of location privacy are inherently unique in character, and spatial data scientists are well-versed to lead this discussion. While a typical conversation on the topic of privacy inevitably turns to the protection of credit cards, bank accounts, or social security numbers, protecting one's location data is arguably more important. For instance, we share other's personal locations, innocuously, without them knowing. Current technologies and tools exist that are so new that we still do not really know what to do with them

(e.g., social media mapping platforms such as *SnapMaps*). Newer generations view these technologies as a standard for social interaction unconsciously making the decision to pay for a monetarily free application using personal data as currency. Lack of awareness concerning the contribution of this location data has led to web applications such as *PleaseRobMe.com* and social concerns such as the tracking of citizens by their governments. For the average person who is not in this predicament, however, location disclosure makes them vulnerable to aggressive marketing and location-based advertising. These techniques and technologies are way ahead of most legal regulations and policy makers are not able to keep up. Finally, advances in artificial intelligence (e.g., tools such as neural networks) have promised to make significant contributions in spatial domains such as autonomous vehicles, feature detection, etc. Again, these advances come with a cost, often increasing the speed and ease with which individuals or groups are identified.

Lastly, a few words on the origins of this special issue. This issue was born out of the *Location Privacy and Security Workshop* held in conjunction with the *10th International Conference on Geographical Information Science* (GIScience) which took place in Melbourne, Australia on August 28th, 2018. The workshop was aimed at facilitating a discussion surrounding current methods and techniques related to location privacy as well as the social and political implications of location privacy, among others. Contributions and discussion at the workshop revolved around methods and techniques for securing location information, following a keynote presentation on the operationalization of differential privacy by Dr. Benjamin Rubinstein [14]. Three papers were accepted to the workshop [13, 5, 12] and all participants were invited to submit full papers to this special issue.

After careful review, two papers were accepted: a novel research manuscript entitled *Exploring the effectiveness of geomasking techniques for protecting the geoprivacy of Twitter users* by Gao et al. [6], and a survey manuscript entitled *Privacy, space, and time: A survey on privacy-preserving continuous data publishing* by Katsomallos et al. [8]. We thank these authors for their contribution to the domain of geospatial privacy and security.

Grant McKenzie
McGill University, Canada

Carsten Keßler
Aalborg University, Denmark

Clio Andris
Georgia Institute of Technology, USA

References

[1] ARMSTRONG, M. P., AND RUGGLES, A. J. Geographic information technologies and personal privacy. *Cartographica: The International Journal for Geographic Information and Geovisualization 40*, 4 (2005), 63–73.

[2] DOBSON, J. E., AND FISHER, P. F. Geoslavery. *IEEE Technology and Society Magazine 22*, 1 (2003), 47–52.

[3] DUCKHAM, M., AND KULIK, L. A formal model of obfuscation and negotiation for location privacy. In *International conference on pervasive computing* (2005), Springer, pp. 152–170.

[4] DWORK, C. Differential privacy. *Encyclopedia of Cryptography and Security* (2011), 338–340.

[5] GAO, S., AND HUANG, Q. Exploring the effectiveness of geomasking techniques for protecting the geoprivacy of twitter users. In *Location Privacy and Security Workshop* (2018).

[6] GAO, S., RAO, J., LIU, X., KANG, Y., HUANG, Q., AND APP, J. Exploring the effectiveness of geomasking techniques for protecting the geoprivacy of twitter users. *Journal of Spatial Information Science*, 19 (2019), 105–129.

[7] GLUECK, J. How to stop the abuse of location data. *The New York Times* (2019).

[8] KATSOMALLOS, M., TZOMPANAKI, K., AND KOTZINOS, D. Privacy, space and time: a survey on privacy-preserving continuous data publishing. *Journal of Spatial Information Science*, 19 (2019), 57–103.

[9] KESSLER, C., AND MCKENZIE, G. A geoprivacy manifesto. *Transactions in GIS 22*, 1 (2018), 3–19.

[10] KRUMM, J. A survey of computational location privacy. *Personal and Ubiquitous Computing 13*, 6 (2009), 391–399.

[11] KUGLER, L. Protecting the 2020 census. *Communications of the ACM 62*, 7 (June 2019), 17–19. 10.1145/3329719.

[12] LIU, X., CHEN, H., AND ANDRIS, C. trajGANs: Using generative adversarial networks for geo-privacy protection of trajectory data (Vision paper). In *Location Privacy and Security Workshop* (2018).

[13] NAGHIZADE, E., CHAN, J., AND TOMKO, M. Seeking Mr & Ms Regular: Sentinels to Characterize Crowd Dynamics (Vision Paper). In *Location Privacy and Security Workshop* (2018).

[14] RUBINSTEIN, B. I., AND ALDA, F. diffpriv: An R Package for Easy Differential Privacy. *Journal of Machine Learning Research 18* (2017), 1–5.