Platform developed to help users control their personal data

June 12 2020, by Melanie Lefkowitz

Credit: Pixabay/CC0 Public Domain

The trove of digital data we generate in our daily lives can potentially

make us more efficient, increase sustainability and improve our health, among other benefits, but it also poses threats to privacy.

To help individuals take greater control of their personal information, a team of Cornell researchers has developed and tested a platform, Ancile, that allows users to set restrictions on what kind of data they'll release, and to whom.

"A lot of data is being collected about us, and we don't have agency in deciding how this data is used," said Nate Foster, associate professor of computer science and principal investigator for the Ancile project.

"The ecosystem around all this additional data has gotten really rich and complicated," Foster said. "So we were interested in developing a systems infrastructure that would let us specify and enforce policies from the individuals' perspective—to sort of invert the control."

This research also offers insight into how contact-tracing apps might protect people from COVID-19 without sacrificing individual privacy.

Passively generated data, such as location, is culled via smartphones' network connections, as opposed to data shared actively through social media posts. Passive data is increasingly being collected and shared by a wide range of third-party applications, from smart building apps that adjust heating and cooling based on how many people are in a room to marketers amassing information on eating and shopping habits.

Ancile was tested with study participants at Cornell's Ithaca and Cornell Tech campuses, with applications that used their location data for practical purposes—but with limits over how precisely or widely that information could be shared. The research was described in "Ancile: Enhancing Privacy in Ubiquitous Computing for Use-Based Privacy," presented at the Association for Computing Machinery's Workshop on

Privacy in the Electronic Society in November 2019.

The team developed location-based apps to demonstrate what's known as use-based privacy, which associates data with policies that authorize certain uses, without allowing unrestricted access. The four apps they developed and tested, each of which addressed a specific privacy challenge, were:

- BookNearMe, to reserve a meeting room based on a user's current location, but with location data blurred;
- RoamingOfficeHours, designed for instructors who want to hold regular office hours at irregular locations, without revealing users' locations outside of office hours or when they're not on campus;
- GroupStudy, to help small groups collaborate in person while hiding all information except whether a quorum of the group is present at the same location; and
- LocationPredictor, which uses machine learning to predict users' next location based on where they are, while preventing location traces from being leaked or used for any purpose beyond the prediction model.

With Ancile, users could specify privacy guidelines that the system would then incorporate—in a reactive rather than static way, because the way information is used changes over time.

"The individuals participating in our studies could say things like, 'I'm OK with my data being used, but only shared with my friends,' or, 'Only share my location information if it's fuzzed within three feet resolution,'" Foster said. "Then applications that wanted to use the data would have to interface with the system."

In developing Ancile, Foster said, the researchers didn't judge whether

certain data uses were good or bad, but simply sought to give users more control over them.

"What counts as a useful system is a very subjective decision," he said. "This is a happy medium where you can still take advantage of data, but in a way that is not infringing [on] the privacy of individuals."

More information: Eugene Bagdasaryan et al. Ancile, *Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society - WPES'19* (2019). DOI: 10.1145/3338498.3358642

Provided by Cornell University