New report analyzes online location privacy

March 1 2010

(PhysOrg.com) -- More and more, the Internet knows where you are. In a new study, three scholars at UC Berkeley's School of Information analyze implications of new online geolocation standards.

More and more, the Internet knows where you are. Smartphone apps recommend nearby restaurants, social-networking sites tell your friends where to find you, and even advertising tries to highlight local businesses.

But revealing your physical location online comes with a potential dark side; it may leave you vulnerable to stalkers or to websites like pleaserobme.com/, and it may reveal more of your private information than you anticipate.

Three I School scholars released a new report today analyzing the [privacy implications](#) of new online geolocation standards. The report, "[Privacy Issues](#) of the W3C Geolocation API", by master's student Nick Doty, assistant professor Deirdre Mulligan, and adjunct professor Erik Wilde, offers feedback on a proposed new standard for the web's geolocation API. As more and more people access the web from [mobile devices](#), the API provides a standard way to access data about your physical location in real time.

"Location is a particularly sensitive piece of information," explained Doty. "Your location reveals details about you that are potentially very personal: where you live, or what doctor you visit, or what you bank you use. And it also opens you to physical intrusion; a stalker — or a police officer — could use this location information to find where you are right now."

Mulligan offered another example. "Remember when Paris Hilton's cell phone was stolen? It revealed all of her calling patterns and all of her friends. Imagine if it also had Loopt on it: it would have told you where all of her friends were. Whoever had her phone would have been able to follow her friends around."

The report coincides with investigations by the US House of Representatives, which has a joint hearing on "The Collection And Use Of Location Information For Commercial Purposes" scheduled for today.

Doty has been working closely with congressional staff who are studying the issue, as well as with members of the Center for Democracy and Technology, who will be testifying at today's committee hearing.

Historically, information about people's physical locations has been subject to a "heightened level of protection" in [privacy](#) legislation,

according to Mulligan. "Think about the advice that parents give their kids: 'Don't tell people your name and don't tell people where you live.'"

The report provides a web page (npdoty.name/location) that demonstrates how the geolocation API works. When accessing the page from a GPS-enabled smartphone, the page can log your exact physical location and pinpoint you on a map. Even from a non-GPS enabled web browser, the page often identifies your general location. The demonstration page — unlike almost all of the sites studied — describes its use of location information in its privacy policy.

"The privacy mechanisms that the API supports will determine the future of how users have their privacy protected," according to Doty.

Doty has been researching standards for location privacy for over a year. "It's been helpful that we have experts in both technology and privacy in the school," he explained. Mulligan agreed: "This is a perfect I School project."

  More information: Report: escholarship.org/uc/item/0rp834wf

Provided by University of California - Berkeley