Location tracking on cell phones raises privacy concerns

September 30 2009, By Troy Wolverton

I love the location-based features on my iPhone. But after talking with privacy advocates last week, I'm concerned about who's keeping track of my location -- and what they're doing with that data.

All new cell phones can track a person's geographic location. Government regulators required the features as a safety measure to help authorities find individuals in the case of an emergency.

But software developers have been able to use that geographic data for many purposes other than just emergencies. Thanks to their efforts, many phones these days can provide turn-by-turn directions, show you the nearest supermarket or track your latest bike ride. I use such features all the time on my iPhone, and I am not alone in seeing the value of location-based services.

Many Flickr users think nothing of posting pictures on the site that identify where they were when the picture was taken. And services such as Loopt and Google Latitude act like a beacon, showing friends -- and potentially anyone else using the application -- where they are at a particular moment.

Such capabilities have caught the eye of marketers and corporations, many of whom have started to build location-based applications for the iPhone and other devices. Pizza Hut, Starbucks, Bank of America and other retailers offer smart-phone applications that can tell users the location of their nearest store, allow them to place an order and even pay

for the order using their phone.

But that's just the first step. Marketers are particularly excited about being able to target ads at particular consumers based on their geographic location.

Imagine getting an ad on your phone from Starbucks offering you $1 off your favorite drink right as you are walking by a Starbucks shop. Or imagine getting discount offers from area restaurants when you check into a hotel.

Marketers argue that such ads would be mutually beneficial for companies and consumers, allowing companies to offer consumers marketing information when it's most pertinent to them.

But privacy advocates such as John Morris, general counsel of the Center for Democracy and Technology, worry that such location-based services are ripe for abuse.

While marketers typically have to get consumers' consent before tracking their location, Morris and others note that consumers are typically asked just once. If they answer "yes" that first time, marketers typically assume they have permission in the future.

Privacy advocates also question whether consumers fully understand how their data could be used. The typical iPhone app simply asks users whether it can "use your current location." It doesn't explain in detail how that information will be used.

Many consumers assume the information will be used by that program just to, say, determine the closest Starbucks. But privacy advocates note that there's little to limit a marketer to just that. There are few rules for what marketers can do with location data they collect.

Standards bodies are working on the problem and have proposed a system in which marketers would have to give much more detail about how they would use consumers' location data and consumers would have to explicitly agree to those terms.

But the protections would be limited. As long as they got consumers to agree to such terms, businesses could still keep the location data for as long as they like, transfer it to other marketers, link it to other databases stored about consumers online or off, and even, in some states, hand it over to law enforcement officials without a warrant.

And getting consumers to agree probably wouldn't be much of a hurdle. Few consumers read through a Web site's privacy policy before using the site, and they'd most likely treat a location privacy agreement the same way.

Yet, location data collection has obvious implications for personal security. With access to that kind of information, a stalker could easily track down a potential victim and criminals could know precisely when to break into people's homes. Those scenarios may seem far-fetched, but the epidemic of identity theft and security breaches in recent years that have divulged Social Security and credit card numbers should raise some concerns about how well marketers will protect location information.

And the danger extends to sensitive information about our health and personal interactions. If I'm regularly showing up at a cardiac surgeon's office, a marketer might reasonably assume I have a heart problem -- information that might be of interest to potential employers and insurers. Similarly, your boss might like to know if you're visiting a competitor for a job interview when you're supposed to be at a conference.

I find all that unnerving. I don't know about you, but I'd like to know where the local gas station is without having to worry that my

movements are under surveillance.

—