Joe Rider
SE 4930
Article Review 1
12/9/11

The topic of the article reviewed was location privacy issues and mobile devices. Mobile devices are able to collect a user's location with a great deal of accuracy. Mobile devices also accompany their owner everywhere which makes the location data very complete. The public and the media were up in arms when it was shown that iPhones were collecting and storing months of location information in an unencrypted format.

The article does indicate that there are benefits to having access to the location data. The main beneficial use of location data is for navigation purposes. The negative side is that location data can reveal much more than just where a person has been. The data can reveal personal aspects such as religious affiliation and where friends live. The article cites a study that shows that past movement data can be used to predict future patterns with 93% accuracy.

The privacy principles are listed as being collection limitation and data minimization. A suggestion is that if location data is necessary, that the accuracy be limited to protect the privacy of the user. The data minimization aspect is that the time frame of data stored on the device should be short, perhaps a few days at the most.

The main point that I took away from this article was the fact that personal information such as location can help to personalize an application. Users need to know and understand what information is being recorded upfront. If people find out that information is being recorded that they were unaware was being used, they are likely to stop using the application.

One of the things that I can apply in future software development is informing the user. If an application is being developed that requires location information users need to be informed in a way that is more effective than just showing a privacy agreement and expecting the user to read it. Another thing is to apply the privacy principles as much as the requirements of the application allow. One way to apply the collection limitation aspect is to give the user the choice of how accurate they would like the location readings to be. The user would be informed that a more accurate reading would make the app more usable but a less accurate reading would protect their privacy more if the data was compromised.

The stored data also needs to be protected with some sort of encryption. I think that the main reason that people were upset over the iPhone situation is that the data was unencrypted

and could be accessed if the device was compromised. Users will be much more likely to share information if they trust that it is protected in some way.

The main question that I had after reading this article was "What is the right about of personal information to have?". I realize that this is application dependent and that often the answer is "the more, the better". If more scandals related to the improper use or handling of personal information occurs, this question will probably be answered in the legal arena.

As mobile devices begin to collect more and more information, the issue of privacy becomes a bigger issue. One the most valuable pieces of information is a person's location history. Application developers who create location-based services need to take into greater consideration how this information will be secured and how the user will be informed that the data will be collected.

## Bibliography

Whalen, T. (2011, November/December). Mobile Devices and Location Privacy: Where Do We Go From Here? *IEEE Security and Privacy*, 61-62.