Use location services and help protect your privacy

It's 10 o'clock—does your phone know where you are? Does everybody else? Chances are that the GPS built into most mobile phones and other portable devices would be able to pinpoint your location within a couple dozen feet.

If you've used your mobile device to map directions or locate a nearby restaurant or cash machine, you've used its GPS.

Phone cameras (and increasingly, regular digital cameras) can also use GPS to automatically and indelibly embed (geotag) in a photo the precise spot where it was snapped. When you text or email a photo to a friend or post it, whether to a photo-sharing site or social network page, that geotag sticks with it.

Facebook and Twitter can also take advantage of GPS on your mobile device by geotagging status messages and tweets. Enlist in that service, and anyone who gets a message or tweet from you will know precisely where you are.

Signing up for a location service like Foursquare or Facebook Places lets you check in as you go from place to place, making it easy to let your friends know where to find you and meet up. Or, choose a service like Google Latitude to track and broadcast your every movement in real time, all the time.

Others can use your location information, too. The applications (apps) you use may sell your location data to advertisers who can serve up ads related to where you are. When you search the Internet from your mobile device, your search engine is location-aware, and may sell this information to advertisers for the same purpose. Certain services, such as Foursquare, track your location to offer discounts at nearby stores or rewards for checking in. Also, parents can engage tracking services to help keep tabs on their kids, but this software could also be used for nefarious purposes—for spying, stalking, or theft.

The risks

There is certainly anecdotal evidence of risk (theft and stalking), but location services are useful and are not particularly dangerous. There are, however, reasons for using them thoughtfully.

In the short term. It's easy to lose track of how much information you're giving and who can see it. There's always the chance that someone you don't want to know where you are, will.

For example, if messages that share your location are tied in with your Facebook account, then your network of friends knows your location. If they're tied into Twitter, potentially everyone in the world could know it. Thieves could also monitor those messages to find out when you're not at home.

Over time. It helps to remember that location information is cumulative, added to the web of other data about you from your phone, social sites and blogs, comments you leave, and so on. It's likely permanent, could be searchable, and ultimately may be seen by anyone on the Internet. Ask yourself how this could affect your online reputation. What would a future employer, university admissions officer, or friend think if he or she came upon it?

How to use location services safely

Choose from among the strategies below to set the level of privacy that's right for you.

Pay close attention to the settings that use your location

- Consider turning off geotagging in your tweets, blogs, or social network accounts.
- On your mobile device, fine-tune the location settings:
  - Consider disabling its location services altogether. Be aware, of course, that this will restrict such features as maps, bus route data, or services that allow you to watch over your children.
  - Use location features in apps selectively. For example, you could turn on geotagging of photos only when you specifically need to mark them with your location. In any event, it's safer not to geotag photos of your children or your house. (Consider switching off geotagging on your digital camera as well.)

Limit who knows your location

- Share your location only with those you trust absolutely. One way to do this in a location service like Facebook Places is to create a separate list of your closest friends. Then use privacy controls to restrict access to location status updates, messages, photos, and the like.
- Disable the option that allows friends to check you in to places.
- Set your location data so that it's not publicly available or searchable.

If you use location services, check in thoughtfully

- Pay attention to where and when you check in.
  - Does it enhance or harm your reputation?
  - Avoid checking in from home, your kids' school, a friend's house, or anywhere you might put others at risk.
  - Think about your safety if you check in when you're alone.
- Link to social media with care. Avoid sending your check-ins to Twitter, Facebook, or your blog.

Help protect kids using location services

- Consider disabling the location features on your child's phone. At the very least, turn it off in the phone's camera.
- Unless you have discussed it with your teens and feel they have the maturity to use these services responsibly, they should not use check-in services.
- Younger children should never meet an online "friend" in person. Teens need to work with parents to create a plan for meeting, like bringing along a trusted adult and meeting in a public place, like a coffee shop or library.

More helpful information

- Get more advice about how to take charge of your online reputation at microsoft.com/protect/privacy/reputation.aspx.
- Find out how to disable location services on many popular phones, including the iPhone and Google Android (Verizon Droids), at ICanStalkU.com.
- Learn about privacy and location services on Windows® phones: microsoft.com/windowsphone/en-us/howto/wp7/web/location-and-my-privacy.aspx.