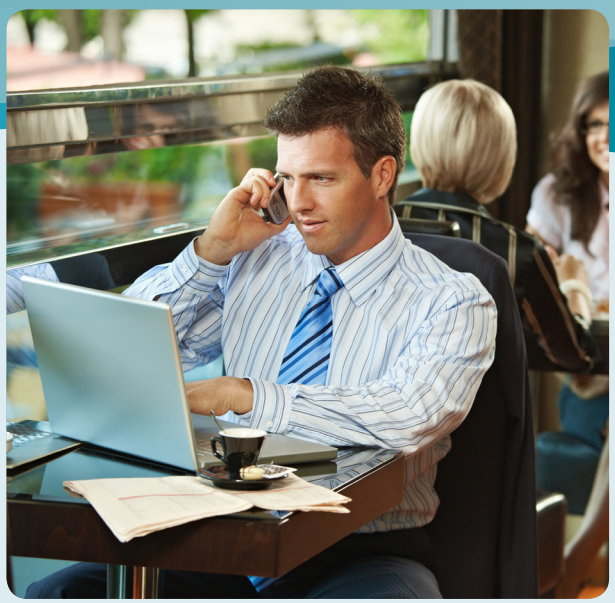
Use Location Services More Safely

Microsoft



In just a few short years, smartphones and other mobile devices have become indispensable given the rich services that help us map directions, locate a nearby restaurant or cash machine, or get local weather. Some of those services rely on unique location data to provide personalized results. This data may be collected through your phone's Global Positioning System (GPS) or through nearby Wi-Fi access points and cell towers.

Your phone's camera can also use GPS to automatically embed (*geotag*) information about the precise spot where a photo was taken. When you text, email, or post the photo—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 posted from it. Enlist in a social network's geotagging service, and anyone who gets a message or tweet from you will know where you are.

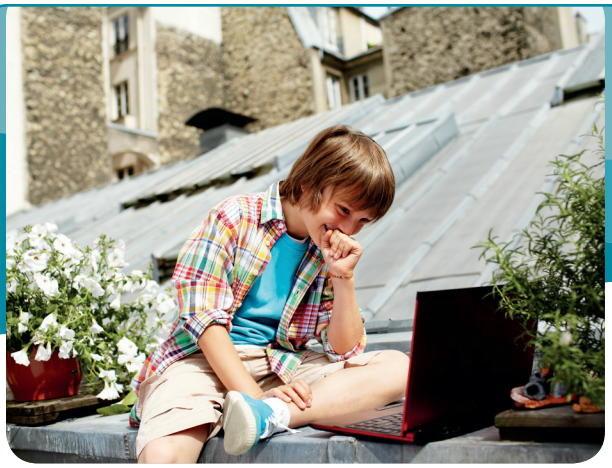
Signing up for a location service like Foursquare or Facebook Places lets you check in as you go from place to place, making it easy to let your friends know where to find you and meet up. Or, a service like Google Latitude will track and broadcast your whereabouts in real time, all the time.

Others can draw on your location data if it's shared publicly. The applications (*apps*) and search engine you use may give it to advertisers who could deliver ads related to where you are. Certain services such as Foursquare track you so they can offer discounts at nearby stores or rewards for checking in.

The risks of using location services

It's easy to see the benefits of location services. But because a person's location in the world is sensitive, there are reasons to use these services thoughtfully.

- Location information is another key data point added to any other data you make public on social sites and blogs, comments you leave, and so on. It is likely permanent, searchable, and has the potential of being seen by anyone on the Internet.
- If messages that share your location are tied to your Facebook account and your privacy settings include a broad network of people, you may be sharing location information with acquaintances and others who shouldn't have access to it.
- If your location-sharing messages are tied to your Twitter posts and you have turned on the "Tweet With Your Location" feature, there is practically no limit to who might know where you are and when you're not at home.
- The same software that parents can use to help keep track of their kids may also be exploited for criminal purposes—spying, stalking, or theft—if location information is made publicly available.



Microsoft

How to use location services more safely

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

Fine-tune location settings

> Think carefully before turning on geotagging in your tweets, blogs, or social network accounts.

> Check your phone settings for any application that uses your location to provide a service. You may have agreed to share this information without realizing it when you installed the app.

> Apply location features selectively. For example, turn on geotagging of photos only when you specifically need to mark them with your location. Note that it's safer not to geotag photos of your children or your house.

> Consider disabling location services on your phone altogether, or limiting the applications you allow to access this information. Be aware, of course, that this will limit features such as maps, bus-route data, or services that allow you to watch over your children.

Restrict who knows your location

> Share your location only with those you trust. For example, when using a service like Facebook Places, create a separate list of your closest friends. Then apply privacy controls to restrict access to location status updates, messages, photos, and the like.

> Disable options that allow others to share your location (check you in) on your behalf.

Pay attention to where and when you check in

Link to social media with care. Avoid sending your check-ins to Twitter, Facebook, or your blog.

> Will checking in enhance or harm your reputation?

> Will it put others at risk? For example, are you checking in from home, your kids' school, or a friend's house?

> Are you alone? If so, is checking in safe?

Help protect kids using location services

In addition to the other ways you can help preserve children's safety online, consider taking these two steps specific to location services:

> Disable the location features on your child's phone.

> Unless you feel that your teenagers have the maturity to access check-in services responsibly, they shouldn't use them.

More helpful info

> Get more advice about how to take charge of your online reputation: **microsoft.com/security/online-privacy/reputation.aspx**.

> Learn about privacy and location services on Windows phones: **aka.ms/location-privacy**.

> Find out how to disable location services on many popular phones, including the iPhone and Google Android (Verizon Droids): **icanstalku.com/how.php#disable**.

> Learn how to secure your smartphone: **aka.ms/phone-security**.

Content contributor LOOKBOTHWAYS ilookbothways.com

1011 PN 098-117535