BRANDPROTECT EXECUTIVE THREAT BRIEF

brandprotect™

April 2015 | Briefing 4

YOU ARE HERE. … AND EVERYONE KNOWS IT!

EXPOSING YOUR GEOLOCATION INFORMATION PUBLICLY CAN LEAD TO INCREASED PERSONAL AND BUSINESS RISK

It is remarkable how freely we tell the world one of the most important things about ourselves: where we are. The everyday use of geotagging and geolocation data has enabled many wonderful things, but other things it has enabled are not so pleasant. From photos of recognizable places posted on social networks, to location check-in apps like Foursquare, Yelp!, or Facebook, **we leave a vivid online trail of our comings and goings**. We often provide our location information to others without even realizing it, for example, when we post photos with embedded geolocation data, use social media services or certain mobile apps with geolocation features turned on, or visit certain websites, we may be accidently broadcasting our location to the world.

WHAT ARE THE RISKS?

There are two basic risks and a host of other smaller ones to posting your geolocation publicly. First, if your location is known to others, you can be met, interrupted, detained or worse. **And if people know where you are, they also know where you are not,** which might put your family, property and other assets at risk. The same is true of your family, your friends and your colleagues. How would you feel if strangers knew where your loved ones were? Remember, with the help of online tools, it's easy for someone to discover your address. Using any of a number of popular real estate applications; it's easy for strangers to have a good look at your house and at your street. Zip codes and job titles easily allow criminals to make educated guesses about your income and net worth. If the criminals know where you live, you may become a more tempting target.

Zip codes and job titles make it easy for criminals to make educated guesses about your income and net worth. If you provide them with your location, you become a more tempting target.

22101	☐	McLean	VA
22102	☑	Mc Lean	VA
22102	☐	McLean	VA

The other "smaller risks" include the possibility that others may infer things about you, your actions, your business and even your allegiance, if they notice where you are, especially if you are in a place where they didn't think you were supposed to be. Think about what your phone records reveal about where you are – and multiply that by 10x or 100x.

WHERE ARE THESE RISKS COMING FROM?

Far and away the most obvious way we reveal our location is through social media posts and uploaded photos. When you check in using Foursquare, you are explicitly telling the world where you are. When you say you are attending an event on Facebook, you are telling the world where you will be and when. **By posting a picture of a nice steak at the Original Morton's places, it'll be known that you are at 1050 N. State St. in downtown Chicago.** Do you want the world to know that? But, even without the useful post identifying your location, it is likely that buried in the photo's data are the numbers 41.901670,-87.628810: the exact latitude and longitude of the Original Morton's Steakhouse in Chicago. The bottom line is that just by examining your photo, people can learn your location.

Your mobile device always knows where you are, roughly determining your location using cell towers and triangulation, and accurately determining your location when your GPS is activated. Of course you know this, as every time you open up your favorite mapping app, the map is centered on your actual location. Even your web browser broadcasts where you are, using information from wireless networks and IP addresses to provide your location to web vendors.

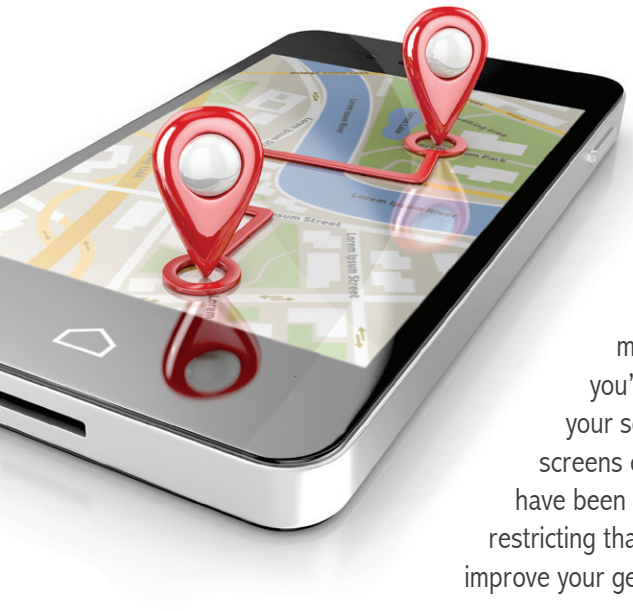
HOW DO THEY KNOW WHERE YOU ARE?

- Observing the locations and activities you post in real time.
- Examining pictures with embedded location data.
- Ttriangulating your position when your GPS is active.
- Stealing your location from the mapping applications you use.
- Intercepting browser and IP data as your use your computer on wireless and local networks.

MOBILE APPS INTRODUCE UNIQUE GEOLOCATION RISKS

It's obvious that to be useful, a mapping application needs to know where you are. But, did you know that many other apps - even gaming apps and puzzle apps – request to have access to your geolocation? Unlike social media posts or photos, which are explicitly created and transmitted by a user, apps on your **mobile device can be constantly on, silently communicating** with their publisher.

When you install a mobile app, you will be presented with a box listing the various permissions that the app seeks. Along with access to contacts, geolocation data is among the frequently requested permission, as is the ability to access the network.



You may be tempted to just click "okay," but if you can, stop and review the permissions and ask yourself these two questions: Do I trust the publisher? Am I happy to let this publisher have this personal information about me and my whereabouts? In most cases, you can still install the application, but you'll want to disable its access to geolocation data in your settings screens. And when you have your settings screens open, review the access that all of your apps have been granted to your geolocation data. In most cases, restricting that access to "when the app is being used" will improve your geolocation security AND increase your battery life!

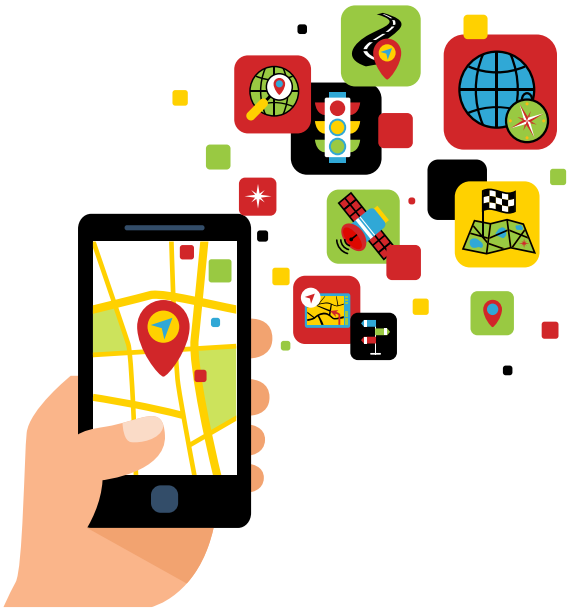
When installing a new app ask yourself two questions:

Do I trust the publisher?

Am I happy to let this publisher have this personal information about me and my whereabouts?

We've come a long way from a world where we deceived our parents with plausible or vague explanations of where we will be (i.e.: Brooks says, "I'm at Sam's"; Sam says,"I'm at Brooks'"). Thanks to GPS, mobile devices and web browsers, it's almost impossible to be invisible. But, by educating yourself on the risks of sharing your geolocation data, **you can take simple steps to protect yourself and your family** from exposure to those risks that arise from third parties knowing your location.

MINIMIZE YOUR EXPOSURE TO GEOLOCATION RISK



How can you minimize your exposure to geolocation risk?

- Be careful about **who has access** to your location.
- **Turn off the geo-tagging** function on your cameras (phone and traditional cameras)
- **Limit social network access to your posts** to just your closest friends
- **Don't announce your location** or your travel plans in posts
- **Delay upload of travel photos**
- Be **wary of cross-network posting** (Facebook/Twitter/Instagram/LinkedIn/other)
- **Review your installed mobile apps for geolocation access** – turn off geolocation access whenever you can

brandprotect™

www.brandprotect.com
sales@brandprotect.com | 1.866.721.3725

For enterprises concerned about their business exposure to increasing online risk, BrandProtect™ provides a complete suite of world class Internet threat detection services to monitor the entire social Internet spectrum and mitigate business risk arising from fraudulent or unauthorized online activity. BrandProtect, helps security, risk management, and marketing organizations at leading financial services institutions, large-scale retailers, insurance providers, telecoms, pharmaceuticals and more, protect their brand value and business bottom line.