The Dark Side of Social Media

Linda becomes paranoid in this article, as she speculates on the darker side of social media and how it could, in the future, "own" its users.

The Good, Bad and Ugly in Social Media

I'm all for social media, especially if you want to build a business, connect with friends and keep your mother happy with a daily virtual hug. But, there are two sides to every coin, and social media also has its down side. In fact, some sides are downright ugly, or could turn ugly for any given person at any moment in time.

I'm not alone in feeling somewhat paranoid about using various social media platforms or with putting all my virtual eggs into one social media basket. In this article, I want to provide you with some information to think about, especially if you're one of those media geeks who wants to try out every new electronic gizmo before anyone else gets their hands on it first.

Location, location, location

Real estate sales people often repeat the mantra, "location, location, location," when pressed about a property's value. Location is everything, and if you are into letting people know where you live, shop, drive and work, then you can become a commodity like real estate.

Recently, PCWorld offered an article that explained why Google's latest location-based feature for mobile devices, which went live recently, will make it easier to find restaurants, bars, ATMs and more when you're in an unfamiliar area. Called "Near Me Now," this tool is available on the Google homepage on your iPhone (OS 3.0 or later) and Android (OS 2.0.1 or later) devices, but only to U.S. users at the moment.

To use this Google tool, you must allow Google to identify your location. In the article, the author states that "Google is not entirely clear on what this means, but I assume the search giant is talking about enabling its My Location feature." This latter feature uses cell towers to locate users rather than GPS (Global Positioning System). In other words, while the cell tower approach is not as accurate as GPS, Google still can know which general neighbourhood you are in at any given time "within about 1000 meters."

I don't know about you, but there are many friends and relatives I try to avoid at all costs. Why am I allowing a complete stranger – let alone a corporate entity – know my location?

Is Google Following You, and – if so – Why?

Later this year, PCWorld questioned location tracking software and began to wonder if this type of software and voluntary activity really is all that good for ordinary citizens. The question occurred when Dan Tynan discovered that iGoogle "gadgets can change / spoof their titles, or even make misleading ones. Someone could write a bad gadget and title it "Good Gadget" or "Gmail" or something else that you trust to try to trick you into revealing your location. The gadget could even re-write its title very quickly to pretend to be a different gadget on your iGoogle page."

In sum, the author now assumes that gadgets showing up in your iGoogle home page cannot be trusted. "If they can be spoofed, presumably they can also be used to capture your personal information -- your Google log-ons, Gmail, Google Calendar, and of course, your physical location. A perfect one-stop tool for stalkers, spearphishers, and cat burglars. Nice."

Yes, very nice, especially when I think about my daughter or mother or other people I care about.

The following feature is purely for advertising, so Google knows how to serve up adds for you based upon your location. But, if certain features can be spoofed or hacked, how do you know that you are completely safe? And, again, why are we trusting corporate entities with our locations?

To Be Totally Private, You Need to Ditch Cell Phone in U.S.

A recent IT World article explains why location privacy is important. One issue involves a business that collects location data and then goes out of business or is acquired. At that point, any agreement you had with the initial company becomes moot. And, it appears that when Internet companies go out of business, their data often is their only "tangible, valuable asset."

What if that information is sold to your health insurance company? What if a your boss gets his or her hands on the information? In one case, the author describes how four NYC cops got fired for being clocked in at work in Manhattan when they were actually at home in New Jersey. RFID (Radio Frequency Identification) E-ZPass data was how they got caught.

But, if you really want to hide from location devices (at least in the U.S.), you really need to stop logging locations on your cell phone – taking us back to that ubiquitous cell tower again. According to the Department of Justice (DoJ), if you use a cell phone, you essentially have "no right to privacy" for the tracking information being logged on your mobile phone, because the DoJ says this information is voluntarily disclosed. "Thus, [the user] assumes the risk that his cell-site usage may be disclosed to law enforcement."

Here are several examples of these location software tools and apps:

- GeoClue: This tool aims to enable integration of location-aware technologies in Linux desktop applications.
- Google Latitude: Use this geo-locator on your computer or phone or both with a photo so people can recognize you if they are looking for you.
- Gowalla: A popular iPhone app that lets people broadcast their locations, find friends, and compete to see who's shown up somewhere the most.
- Foursquare: You can go exploring, much like Lewis and Clark and bombard everyone with your location and your status on Foursquare. I mean, everyone.
- Quova: One of several "geo-location" software companies that let Web sites know where users are geographically.
- Yelp: An example of a "soft" location finder, which puts you in a specific location as you visit or wander around your own neighbourhood.

The Center for Democracy and Technology states, "And just to round things out, the Justice Department offers up this no muss, no fuss solution to this privacy quagmire: 'One who does not wish to disclose his movements to the government need not use a cellular telephone.'" Allow me to explain why they say this – I visited our local police dispatch recently and discovered that individuals in dispatch can find you simply when you use your mobile device – within seconds – if they know your number and especially when you call dispatch directly from your mobile device. Seconds – that's all it takes.

If you don't want big government or corporate entities to know where you live or if you don't want them to know about your daily routine, you might think about backing off some social media as well as the tools that use those networks. You may also ponder a few things like liberty, freedom, and use a bit of healthy doubt about how the world is turning right now to contemplate your future use of these tools.

Some Positive Aspects to Location Awareness

This ability to find you immediately through a mobile device is a great thing if your kid gets lost in the woods. Always send your kid out with a mobile device and the number to a local police dispatch unit for his or her

safety if you worry. And, if you haven't committed any crimes lately, and you don't care who knows where you are located, then carry as many mobile devices as you want.

You also can be protected against credit card fraud, as some geo-location software helps to identify users from areas with high instances of credit card theft. If a merchant receives a card from a high-risk area, they can ask the card holder for additional information to verify their identity. Also, if a card was used by two users in different time zones at the same time, a red flag would be raised. But, if you don't use credit cards, there's no need to worry.

That's all I can think of on the up side, other than helping to make yourself feel important as you bombard friends, family and total strangers with your Foursquare locations. How much do you think we care about where you are at any given moment, really? At the same time, how much attention do you think you're drawing from people you don't know – especially if you don't want them to know where you are located?

How to Avoid Oversharing without Paranoia

In February this year, Lifehacker asked their readers about how many of them used geo-location software. It seems that users are in the minority, but to view all the locations that are shouted out on Facebook and Twitter, I think some people are lying. In that article, they mention the Web site, Please Rob Me. This site tried to point out that sharing a location can be an issue, especially if you are sharing where you vacation and that the house is empty.

While that Web site has stopped sharing Tweets from people who use geo-location software, they continue to try to raise awareness about "oversharing" information about your location and other pertinent clues about things such as how much money you have, what type of car you drive and more.

Take a look at the two links displayed on the home page of Please Rob Me. One points to a page at the Electronic Frontier Foundation, which lists many systems that we might use every day that track our locations. While this article also lists some solutions to protecting an individual's identity, they admit that many corporations and communications systems penalize any resolution with higher prices and other issues. This, to me, is one warning sign that a proliferation of location devices is exactly what corporate entities want. While this desire on the corporate level might be "ok" if corporations were limited in power, it becomes an issue when corporations become stronger than governments – such as when French water companies almost took over the French government (see: Blue Gold) and as BP flexes its muscles in the Gulf of Mexico in the ongoing oil disaster.

Even now, there is talk on Capital Hill about the ability of the government to control the Internet to the point where it can "shut it down" in case of a national emergency. When you begin to understand that a supposed "democratic" government is talking about shutting down communication lines – yet possibly have the ability to confiscate location information – then you might think twice about voicing opinions and locations online. At that point, a "free" country no longer is "free," and a person's past can come back to haunt him or her.

In the other link on the Please Rob Me page, which points to the CDT again and an article about over-sharing, the author states, "Social networks have increased enormously in size and number. Most of them allow you to relay messages between different sites and it's easy to lose track of just how much information you might be giving away and how many people have free access to it." This statement leads back to the point that you might want to limit your social media use and how you connect that data, and also the need to stay on top of ever-changing privacy controls within those social networks.

Outside of dropping out, that advice is about all you can use to control what people know about you – except, of course, for what you say. Even talking about the temperature outside might lead people to learn where you are located, especially if they really want to find you. Think ex-spouses, the tax man and other individuals you would prefer to avoid.

Another way to keep yourself somewhat 'safe' is to avoid putting all your eggs into one basket. For instance, I've noticed lately that Google seems to be everywhere, doing everything. Why, then, would I feel the desire to put myself in Google's path, when other options are available, such as Facebook, LinkedIn or Twitter. Of course, the possibility exists that Google could acquire any one of those social networks, but – until then – I can enjoy Google's tools without being enveloped totally by them.

Conclusion

I'm not that paranoid about location information, but I do try to be careful. After all, I have family and loved ones that may be hurt if I become downright stupid about my behaviours online. In the movies, the Mafia doesn't want to hurt you to get information – they would rather hurt your family first, as you might buckle under the latter threat much easier than you would under the threat of personal harm.

So, when you think about corporations and businesses who will soon know where you are at any given time and even how much time you spend in a given location, you might realize that it wouldn't take much for other entities to learn this information as well. Although some Web gurus applaud the progress of software that displays this information, I wonder if those individuals are the same ones who jump into using any software new to the market without thinking first whether or not this software is fully developed, safe and free from malware or hacking.

What? No software is immune from malware or hacking? Maybe I'm not being so paranoid after all.