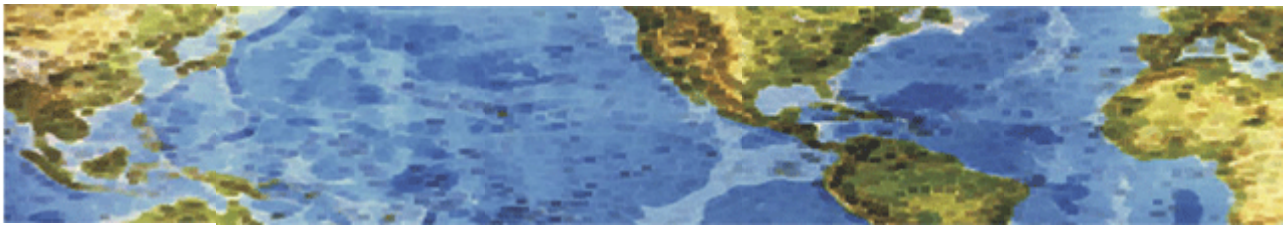
HALL ASSOCIATES



Risk-Based Decision Making Commentary
1 May 2013 Newsletter

What Does the Internet Know About You?

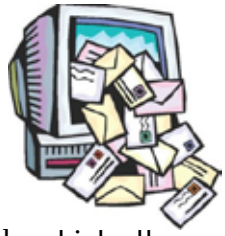
The Internet is a place for people, companies and criminals to pick up more information about you. That includes your address, gender, date of birth and, with a little sleuthing, your Social Security number and credit history. That's been made clear in a recent spate of "doxing" (document tracing) of celebrities that revealed, for example, that Microsoft CEO Bill Gates had an outstanding debt on his credit card. But none of this information comes from hacking. It's either already public or accessible by, for example, paying an online people-finding service to get a Social Security number, and then running a credit check.

Then there's all the data that gets poured into social media sites such as Facebook, Twitter, Tumblr, Instagram, Foursquare and others. Now employers can fire workers for expressing opinions they don't like, strangers can stalk you with mobile apps, cybercriminals can steal your identity or company accounts and college administrators can judge the quality of applicants by the number of drinking photos posted to their account. **People need to understand** that their information has secondary or tertiary uses. The issue isn't so much that information is out there and people can see it. The issue here is when that information gets used in new and different ways. **It's all public.**

Many gun owners felt a secondary use of private information when they saw an interactive map published by the Journal News of White Plains, N.Y., that listed the name and addresses of everyone in two New York state counties with a gun permit. However, the records are all public. There is no current law against publishing them either in print or online, even if it makes some uncomfortable. Of course, some states are rushing to create laws against this practice **for some information.**

When real estate search site Zillow.com first came out, many people were shocked at the amount of information on it — including their physical address, aerial house photos and the price paid for their homes. Last year, Zillow began listing homes going through the foreclosure process, which caused another firestorm of people looking to opt out. But all the information comes from public records. Zillow says it doesn't list names, only properties; and it does not allow those with foreclosed property to "opt out" of being published.

HALL ASSOCIATES



Social oversharing

The Electronic Frontier Foundation cautions about the use of Facebook Graph Search, which allows users to search information from news feeds of friends and those users with settings set to public on Facebook. Now anyone can look for, for example, single women living in San Francisco who share their taste for tapas and perhaps find a phone number and email address. Who needs Match.com anymore?

Today, people's futures are in peril every time their boss or college admissions office looks on the Internet. That means users shouldn't post photos of themselves with an alcoholic drink in their hand or espouse extreme political views, because it can lead to a value judgment. You can still go online and say what you want, but be aware that anything electronic is forever and could go viral. Another problem today is social networks becoming a larger part of one's life. To comment on articles, people frequently log into a Facebook account first. Others are finding that their Google+ social account is being attached to their Gmail account and will be needed to comment on apps or games on Google Play. Google+ accounts are also used to sign into YouTube and other Google sites. Many social networks are seemingly trying to end anonymous posting. To preserve privacy, a person would have to walk away from Google or Facebook. Recently Facebook Home was launched on Android devices, and many noticed that the interface logged online purchases and visits, although Facebook said that it doesn't assign names to the information. Facebook is using customer loyalty cards' information and public records to sell to advertisers and marketers. However, Facebook Home isn't hunting anyone down to do this; people themselves are opting to use an Android phone with the Facebook skin on it.

What you can do

Long-term solutions could be legal, regulatory or even codes of conduct for companies. Meanwhile, users can save themselves some headaches **by understanding that whatever they place online will stay online.** Nothing online is temporary; instead, it's more like an Internet tattoo. Keep all social networks set to the highest privacy settings even if you have to manually approve follow requests. If posting to a forum or other online database, don't use your real name or email address (or at least one you don't mind people seeing). **Never give out** your date of birth, phone number or physical address if you can help it. **Never give out** your Social Security number. Many colleges, banks, brokerage houses and other companies now have alternative login IDs to use provided you ask for one. (However, not even colleges or banks are immune to hackers, so always monitor your credit for suspicious activity.) Remember that what you post can be seen by others. Be careful of what you say and which photos are posted because it could potentially be seen by millions of people.

http://www.technewsdaily.com/17886-what-does-internet-know-about-you.html?cmpid=520751