Leith Wheeler
INVESTMENT COUNSEL LTD.
Well Into the Future

Fall 2013

Planning Matters

Family Security and Social Media

Introduction

Privacy has been redefined.

Despite the benefits, social media has caused an erosion of privacy, leading to greater family vulnerability, exposure, and risks. Today's social media users disclose a vast amount of personal information that can easily go astray, have unintended consequences, and could even be used against them. Families should recognize this new reality and work diligently to establish and maintain online privacy – especially families of wealth.

Social Media and Social Networks Defined

Social *media* is defined as an online platform for sharing information and connecting with others, and typically includes any internet-based platform where people engage in direct dialogue with one another.

Social *networks* take it a step further, creating groups of individuals linked together by a common interest, purpose, or friendship. The growth of social networks has been prolific. The largest social networks are Facebook, Twitter and LinkedIn. Many parents and children alike are a part of one or more of these social networks.

Rapid Growth and Global Reach

The reach of social media is vast and global, and both social media and social networks continue to grow at a rapid rate. As of August 2013, member counts were as follows:

Facebook	1.15 Billion[1]
Twitter	500 Million[1]
LinkedIn	238 Million[1]

Social media has become an inseparable part of the everyday lives of a significant segment of the population. At the end of March 2013, Facebook says it had 665 million active users daily.[2]

Twitter is used as a knowledge-sharing platform, a news vehicle, an election campaign tool, a place of connection for people with every imaginable interest, an arena where celebrities and their fans can connect, and an outlet that gives people a voice. Twitter has 135,000 new users signing up every day. These users "tweet" an average of 58 million times per day.[3]

LinkedIn is a social networking site for business professionals. Even though information is shared on LinkedIn, it does not pose the same security risks as Facebook or Twitter because it doesn't lead users to disclose such a vast amount of personal information.

The increased time spent using social media, its widespread adoption, and the accessibility of information on the internet makes information security an increasingly pressing issue.

Each of these social networking platforms poses varying degrees of risk that must be considered when discussing family security.

Risks, Vulnerability and Security

In an age where change is so rapid, it is easy to adopt new technologies without considering the consequences. Social media have safety and security issues most people don't fully understand.

And of course each family and individual will have varying risk tolerance levels, and will need to determine what level of exposure they feel comfortable with and how much value they place on privacy and protection. Having a conversation with your family surrounding family security and social media is a good place to start, and the following points may be helpful:

1. Disclosing Your Location

Status updates and wall posts on Facebook can inform the world of where you are, or where you will be.

Many users post status updates about vacation plans (inadvertently) letting everyone know the period of time when their family will be out of the house for an extended period of time. This creates a perfect opportunity for burglars and other criminals interested in compromising the family home.

In addition, Facebook is constantly updating and reinventing itself and it can be difficult to keep up with all of the changes. Facebook created a location-based feature which over time has become increasingly automated. Its purpose is to let users easily share where they are, and help them keep track of their friends. The service also allows friends to "tag" friends at a location. Facebook is going to use the service to offer local deals, discounts and rewards to users.

However, many people are unaware of Facebook location service and what it entails. Facebook users are automatically opted-in to Facebook location service -- it's running automatically unless a user chooses to turn it off. And while Sam may not directly use Facebook himself, a "friend" (Susan), if the right privacy settings have not been selected, can broadcast Sam's location to the entire social network of both Sam and Susan.

2. Inappropriate Photos and Tagging

"If you're not comfortable with your activity being on the front page of the newspaper, you probably shouldn't do it." This old adage would be well applied to social media, particularly, Facebook.

Families should discuss parameters surrounding the posting of pictures to social media sites. The following questions provide a good starting point for discussion:

- Are you comfortable with your children posting certain photos of you from family vacations or weekends at the cottage?
- Are your children posting photos from around your home that, likely mistakenly, could let everyone know your home address or the kinds of possessions you own?
- Do your children realize that potential employers often find ways to access Facebook profile pages to review all the information posted, including pictures?

Photos can be harmful, whether they are photos posted by you or a friend. They can be unflattering, embarrassing, or something regrettable that one would rather forget. Families need to be proactive in protecting the privacy of the family – parents and children alike.

3. Detailed Personal Information

A Facebook profile page (specific and unique to each user), holds all the information a user chooses to share. Basic information includes: current city, hometown, postal code, neighborhood, residence, room number, sex, birthday, relationship status, interests, political views, religious views, and a chance to share a small biography and some favourite quotations.

These items appear fairly innocuous, but they may not be. Birthdays are essential numbers, often used for credit card applications and security questions. Hometown and Current Locations are also commonly used as security questions, often in online banking. Allowing the world easy access to such information may be not the best idea. Instead of posting your full birthday, just post the month and day (excluding the year). That way, you'll still receive a raft of birthday wishes, but hopefully protect security information.

Instead of posting your exact current location or hometown, try to post a region (be vague), or just don't post anything at all. Those who are important to you already know where to find you.

Furthermore, Facebook users often have "friends" in their social network they hardly know, or met briefly years ago. If you, or your children, don't know their "friends", delete them. Going forward, friend requests should be screened. If you don't know them, they shouldn't have access to your personal information.

4. Posting Your Information Forever

Forever is a long time. Given the real-time nature of Facebook, information that is shared can often not be taken back. Once it's up, someone has likely seen it and it can be copied and distributed to stay on the internet forever.

If Phil posts a picture of Jay partying on a Friday night, Jay can simply "un-tag" himself from the photo, removing the photo from his profile. But that doesn't remove the photo from Facebook. The photo is still on Phil's profile page. Phil's network can still see the photo of Jay's legendary Friday night karaoke antics.

Oftentimes, social network users, especially young adults and children, tend to act differently online than they would in a face to face scenario. People are emboldened online, and can more easily act in a hurtful manner. The problem is, everyone within your social network (and we have to assume that some people beyond that) can see what you are posting.

Even if someone chooses to share something mean or offensive, it is probably not a good idea to broadcast it to the world. Before posting on Facebook, or Twitter, it is a good idea to consider that most information is there for the long term.

There is a significant shelf life to our online lives.

Privacy Settings

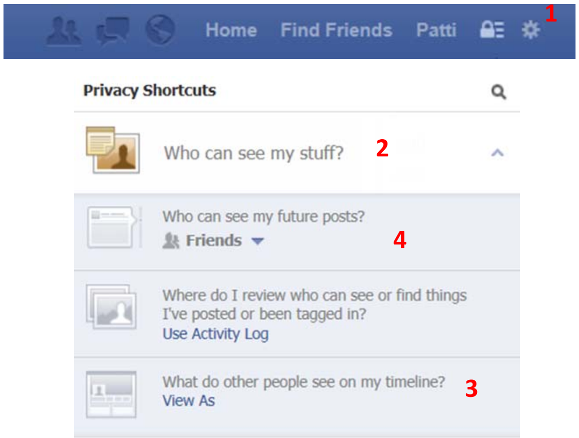
Privacy Settings exist to provide users with additional protection. Unknowingly, you are more than likely sharing information that can be viewed well beyond your "friends" or network connections. In fact, if you haven't specifically chosen to keep your information private, third party applications have complete access to your Facebook profile.

Unfortunately, social media doesn't make the need for, or the selection of, Privacy Settings very clear. If you want to make your information more secure and private, the following steps will help you in that endeavour.

With Twitter, under your Username in the top right corner, select Setting. Simply choose "Protect my Tweets", and only your followers will be able to monitor your updates.

Unfortunately, Facebook is more complicated. Here are a few tips to make your Facebook page more private. To begin, it will be useful to see what the general public can see about you.

On your Facebook homepage, click the small lock in the upper right hand corner (1). Select "Who can see my stuff" (2) then "What do other people see on my timeline?" (3) Click "View As." Now you can see what others can see about you.



Who can see my stuff?

Who can see my future posts?
Friends

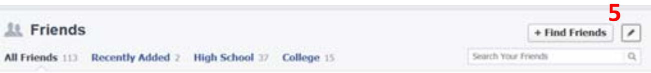
Where do I review who can see or find things I've posted or been tagged in?

What do other people see on my timeline?

First — Look for the statement "To see what she/he shares with friends, send him a friend request." If you see this statement, you are only sharing with friends. If you don't see this, likely the general Facebook public can see your information. If you only want your "friends" or "close friends" or "family" to see your posts you can change this setting in the drop down box marked (4).

Second — If you can see a section called "Friends" hover your mouse over the picture of one of your friends. You will see a message that allows anyone with a Facebook account to message one of your friends. If you don't want 1.15 billion Facebook users to have that privilege then go to your profile screen (find this by clicking on your name in the upper right hand side of the blue bar) and click on your "Friends" tab. You will see a small pencil beside "Find

Friends”(5). Click on the pencil and then click on “Edit Privacy”(6). Change “Friend List” and “Following” in the drop down box on the right hand side from “Public” to “Friends”

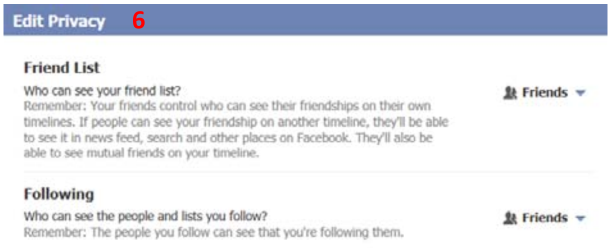


Friends

+ Find Friends

All Friends 113 | Recently Added 2 | High School 37 | College 15

Search Your Friends



Edit Privacy

Friend List

Who can see your friend list?
Remember: Your friends control who can see their friendships on their own timelines. If people can see your friendship on another timeline, they'll be able to see it in news feed, search and other places on Facebook. They'll also be able to see mutual friends on your timeline.

Friends

Following

Who can see the people and lists you follow?
Remember: The people you follow can see that you're following them.

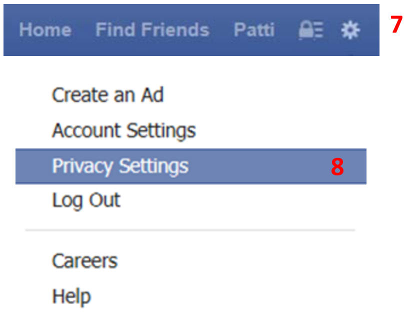
Friends

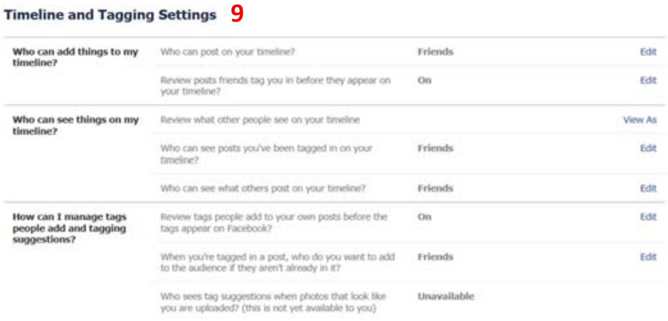
Timeline and Tagging Privacy Setting

This lets you control who can post on your timeline and even allows you to review photos that you are “tagged” in before they appear on your timeline.

In general these settings should be listed as “Friends” rather than “Everyone.”

Find this section by clicking on the settings icon that looks like a little cog wheel in the upper right hand side (7). Click on “Privacy Settings”(8), and look for “Timeline and Tagging”(9) on the left hand side of the page. Click this. Once you are there you can edit as appropriate in the different sections.





Timeline and Tagging Settings

Who can add things to my timeline?	Who can post on your timeline?	Friends	Edit
	Review posts friends tag you in before they appear on your timeline?	On	Edit
Who can see things on my timeline?	Review what other people see on your timeline		View As
	Who can see posts you've been tagged in on your timeline?	Friends	Edit
	Who can see what others post on your timeline?	Friends	Edit
How can I manage tags people add and tagging suggestions?	Review tags people add to your own posts before the tags appear on Facebook?	On	Edit
	When you're tagged in a post, who do you want to add to the audience if they aren't already in it?	Friends	Edit
	Who sees tag suggestions when photos that look like you are uploaded? (this is not yet available to you)	Unavailable	

Contributing Writers:
Tom McCullough
Chairman and CEO
Northwood Family Office LP

Co-Author, *Family Wealth Management: 7 Imperatives for Successful Investing in the New World Order*

Patti Shannon, CFA
Vice President,
Portfolio Manager

Editor:
Patti Shannon, CFA
Vice President,
Portfolio Manager

Views expressed are the views of the contributing writer and do not necessarily represent the views of Leith Wheeler, and do not constitute legal or other advice. Leith Wheeler Investment Counsel Ltd. is an employee owned firm providing portfolio management services for individuals, pensions and foundations. Planning Matters is not intended to provide investment advice, recommendations or offers to buy or sell any product or service.

[1] Expanded Ramblings (August 2013) How Many People Use the Top Social Media, Apps & Services? http://expandedramblings.com/index.php/resource-how-many-people-use-the-top-social-media/
[2] Facebook Growth in the Past Year https://www.facebook.com/media/set/?set=a.10151908376636729.1073741825.20531316728&type=1#!/photo.php?fbid=10151908376726729&set=a.10151908376636729.1073741825.20531316728&type=3&theater
[3] Statistics Brain, Twitter Company Statistics 05/07/2013 http://www.statisticbrain.com/twitter-statistics/

Leith Wheeler
INVESTMENT COUNSEL LTD.
Well Into the Future

1500 — 400 Burrard Street
Vancouver, BC V6C 3A6
Phone 604.683.3391

570 — 1100 1st St. SE
Calgary, AB T2G 1B1
Phone 403.648.4846

Toll Free 1.888.292.1122
LeithWheeler.com