



ERIN POWER

Intern, 2008-2009

**Sheldon Chumir Foundation
for Ethics in Leadership**



Facebook CEO, Mark Zuckerberg

Founded in 2004 by former Harvard student, Mark Zuckerberg, there is now an estimated **175 million** Facebook users!

Facebook, like much of the Internet, is a great innovation -when used properly, the benefits of social networking sites can be very worthwhile.

Crafting your unique cyber identity through self descriptions, pictures, online communities and groups can dominate much of your time. Other than a personal social gateway, the entrepreneurial mind or social activist can use this online tool to their benefit by marketing products or promoting charitable causes. However, we need to pay attention to some ethical and legal issues raised concerning privacy and over-exposure of information.

PRIVACY AND YOU

1. THE BALL'S IN YOUR COURT

**2. WHO HAS ACCESS TO OUR INFORMATION?
HOW? WHY?**

**3. THINKING ABOUT THE MORAL AND LEGAL
CONSEQUENCES**

1. THE BALL'S IN YOUR COURT:



Do most people use privacy settings?

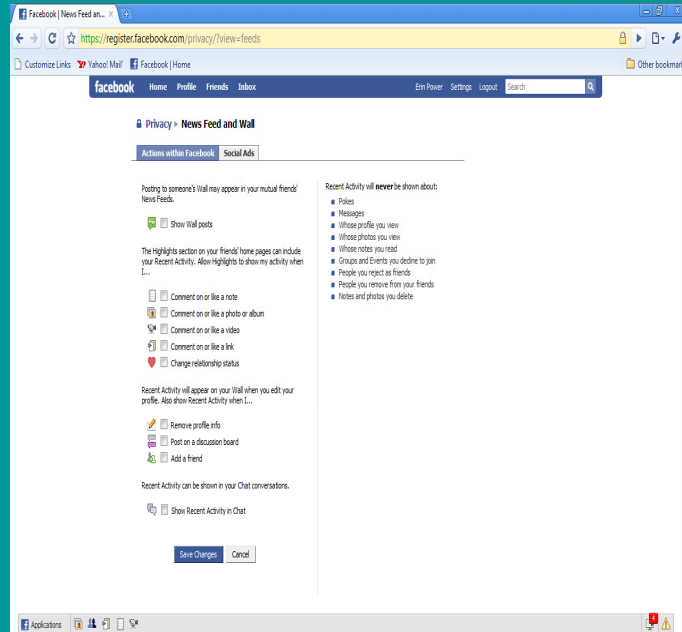
Are you aware of them? Is this an issue?

In my experience, when Facebook does fairly substantive interface overhauls, revamps privacy policy, privacy settings have been reset to default settings - 'open' - and users are not notified. Check them again to be sure you have them set to the tightest settings – to your friend lists or on customized settings. As of this week, Facebook widened the scope of information accessibility by creating an 'EVERYONE' button – you can now share your profile with 175 million people!

THERE ARE TWO WAYS TO CONTROL PRIVACY SETTINGS:

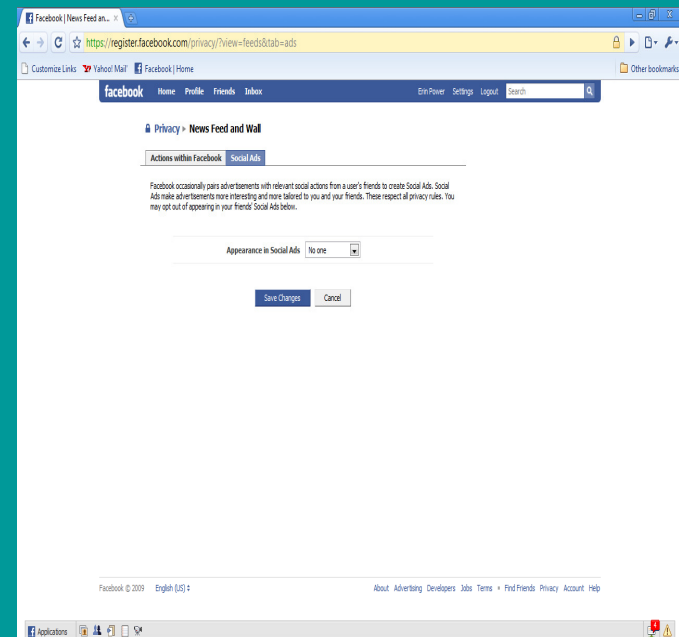
(1) Actions within Facebook

(Profile, Search, News Feed/Wall, Applications pages)



(2) Social Ads

(A consent question)



There are four settings pages to manipulate – it is highly recommended to limit the scope of information accessibility to your friends list or customize further. Broader networks leave your information open to employers, teachers, and strangers who happen to be in your network or beyond. You can also adjust the search page and set the search capabilities on yourself; when your name is searched, e.g. a prospective employer, you can avoid being found on Facebook.

It is also worthwhile to adjust the 'social ads' to 'No-one' as Facebook enjoys distributing your posted information to marketing companies and used at their discretion.

2. WHO HAS ACCESS TO OUR INFORMATION?

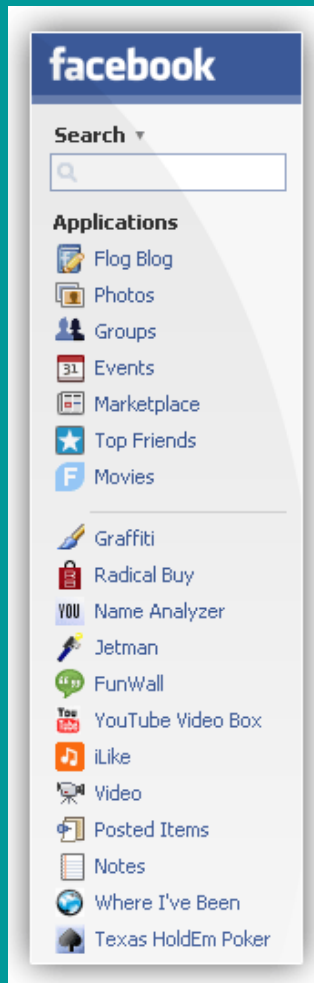
A.) Facebook

In its User Agreement, Facebook states:

“By posting user content to any part of the site, you automatically grant ...

the company an irrevocable, perpetual, non-exclusive, transferable, fully-paid, worldwide license ...

to use, copy, publicly perform, publicly display, reformat, translate, excerpt, (in whole/part) and distribute such user content for any purpose.”



B.) Third Party Applications:

Install an application, (iLike, Scrabble, IQ tests, Gifts, Groups, etc.)

= grant full privileges to your Facebook information.

What does this mean?

Application owners can see what you can see. They can request information about you, your friends, and your network members to use at their discretion.

The Facebook Terms of Use agreement tells application developers not to do this, but Facebook has no way of finding out or preventing this.

Do applications even need this information?

8.7% of applications didn't need any information

82% used public data to function properly (name, network, list of friends)

only **9.3%** needed private information (e.g., birthday).

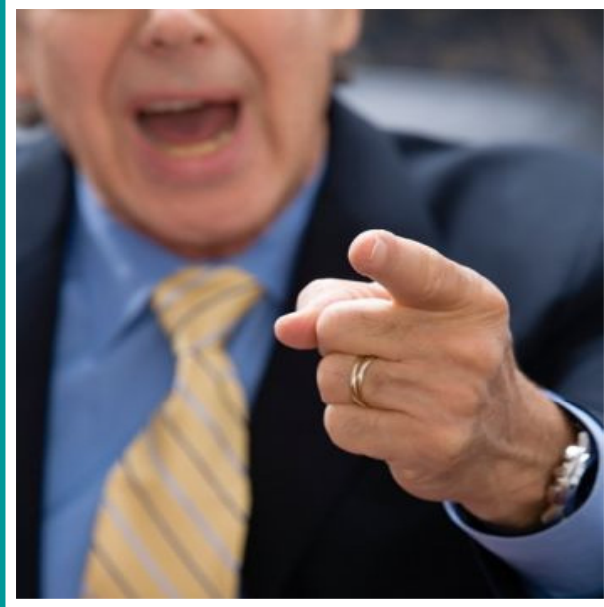
Since *all* of the applications are given full access to private data, this means that **90.7%** of applications are being given more privileges than they need!

A slight exaggeration...



C.) Facebook and your Boss:

According to online statistics, roughly **35 percent** of employers view social networking profiles of candidates as a supplementary background check!



This is a reported statistic (as are similar statistics which reflect profiling online content of *current* employees). However, many employers likely do not report their monitoring behaviour leading researchers to speculate the percentages to be much greater. In most cases, this is not an illegal and is often endorsed as an unofficial hiring screening practice. So, displaying personal information in a public sphere must be treated as something appropriate for public viewing: this is the general business/corporate sentiment. Canadian Privacy Commissioner, Jennifer Stoddart, firmly believes a company's reputation trumps employees' control over their personal cyber content – even if employees are off the clock.

IS THIS EVEN LEGAL?

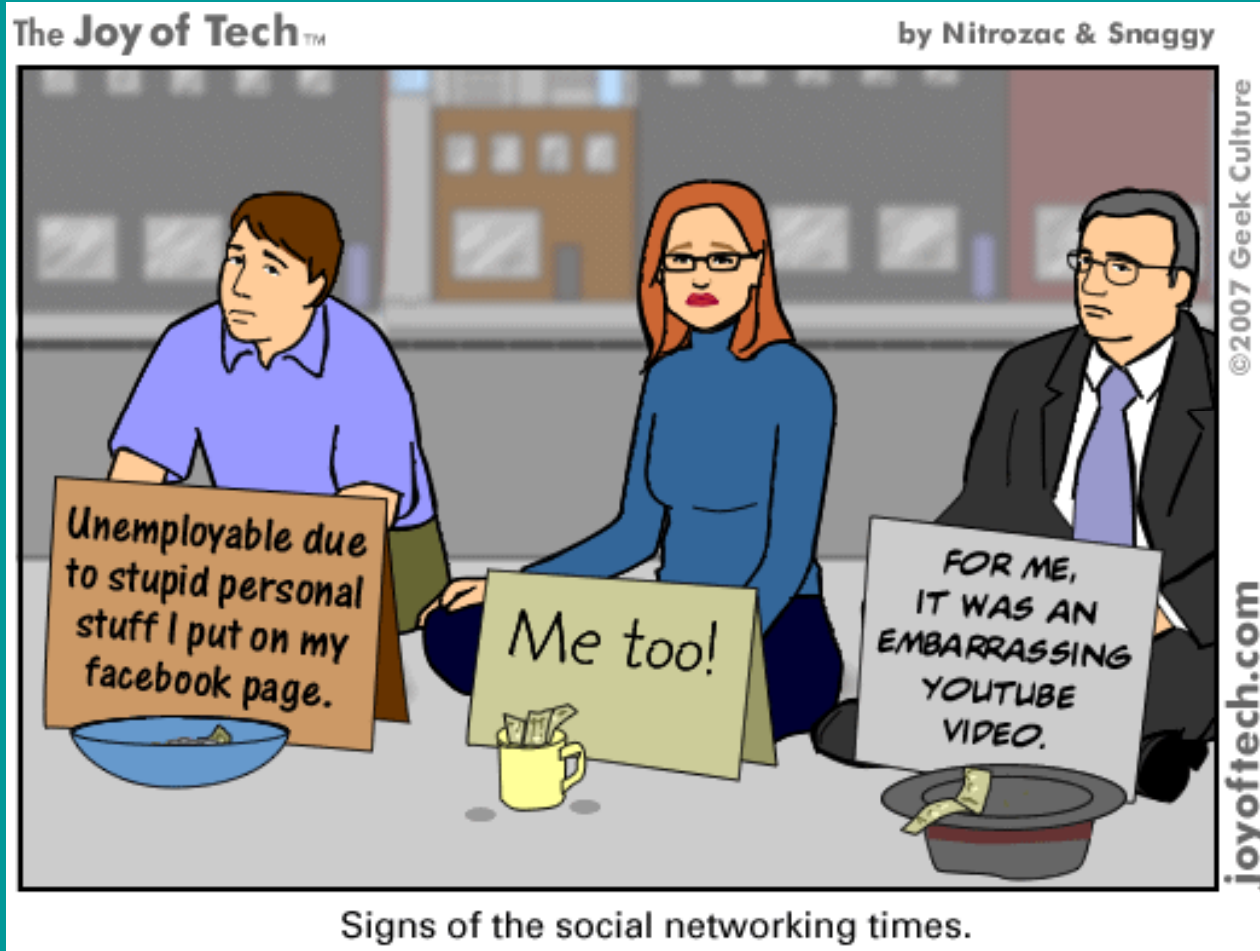


In general, sure, since we are assuming employers view open profiles. However, there could be strong evidence involving employer hacking of privacy barriers (Privacy Law) or unlawful discrimination on the basis of profile information (Discrimination Law).

In general, sure, since we are assuming employers view open profiles. However, there could be (and have been) legal cases made, yet be quite difficult to prove unless, e.g. there is strong evidence involving employer hacking of privacy barriers (Privacy Law) or unlawful discrimination on the basis of employee profile information (Discrimination Law).

- ◆ Remember: **the internet is public. A curious employer coupled with your open profile yields a goldmine of information.**
- ◆ Should **‘accessibility’ = ‘opportunity’** here we’re referring to an ethical question: **“Ought employers be doing this?” We know that they CAN and ARE.**
- ◆ So, it’s clear that **USERS** can at least take some preventative measures to avoid character profiling.

Don't let this be you!



3.) PRACTICAL IMPLICATIONS

FOR STUDENTS!

There have been many documented cases of students posting derogatory comments about principals, teachers, staff and facing school suspensions and lawsuits.

-Some post-secondary institutions judge applicants on the basis of their online social networking profiles – even more reason to use your privacy settings and be selective about what you post!

Examples:

-Morgan Shaw-Fox, Portland Oregon, Lewis & Clark University. Friends of supposed sexual assault victim created Facebook group entitled: “Morgan Shaw-Fox is a piece of s--- rapist.”

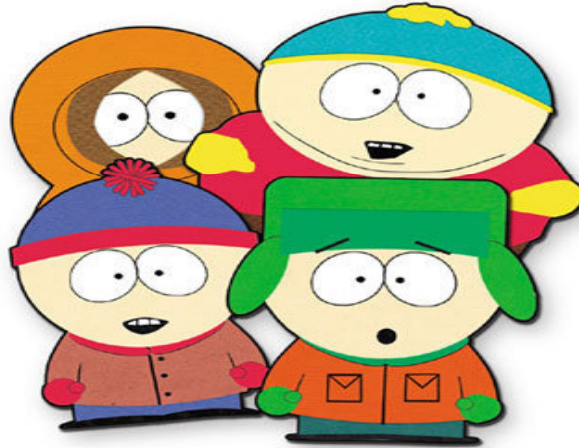
- Stacy Snyder, Millersville University, Pennsylvania, denied her education degree in connection with a drinking photo with the caption, ‘drunken pirate,’ on MySpace

Do you remember?

Facebook and 'Kick a Ginger' Day

Motivated by an episode of the satirical cartoon, Southpark, Facebook groups emerged entitled such things as

'National Kick A Ginger Day, are you going to do it?'.



Some grew wildly popular in Canada/U.S., boasting as many as 5,000+ members and on November 20, 2008, cyber-bullying manifested into real violence.



Identity Theft

-Online predators: ongoing issue

-Acquaintances: taking online content to establish fake networking accounts

e.g. Two Boston, MA, High School students created a fake profile on behalf of female classmate in order to post offensive language and slander her reputation. Criminal charges involved for identity fraud with intention to harm.



Thoughts? Comments?

Privacy concerns?



Sexual Profile Content , Youth , the Law:

In Canada, anyone who publicly posts/distributes sexually charged photos of someone under 18 years, even with their consent, can be criminally charged with **child pornography**. Without consent, the charges can be more severe because they could involve identity fraud and intent to cause harm.

Underage people who engage in '**sexting**' (cell phone transmitted) beyond a 2-person private exchange, can also be charged with child pornography.

At least 39 percent of underage U.S./Canadian youth have been involved in the above activities.

In the U.S., you can be jailed, sent to rehabilitation and are often registered as a **sex offender** in such cases. According to American criminal code, juveniles are treated no different than adult pedophiles.

Thoughts on this?

WHAT NOW?

1. **Privacy settings – Use them!**
2. **Keep your information, postings and pictures sensible and avoid overly personal/offensive content.**
3. **Rule of thumb: Post for Parents/ Teachers/ Managers - sorry!**



4. **Reality: privacy does not exist on the internet**
5. **Enjoy the benefits of social networking!**

