

Online reputation management

Protecting yourself...from yourself (and others)



By Tony Wilson

A good name can be worth millions, and we all know by now what happens when a good name gets into bad trouble. Tiger Woods is only one example of how important your reputation is, and how easy it is to be damaged. Perhaps irreparably.

The online world has created a new area of law in this age of Web 2.0. It's called Online Reputation Management Law, and it straddles the law of defamation, freedom of speech, privacy law, copyright law, and trademark law. It also involves the non-legal (but equally as important) fields of public relations and crisis management. Many of the legal issues in this area involve Facebook, which has over 350,000,000 users, (including about 90% of all the middle school and secondary school students you and your colleagues teach every day. You might be a Facebook user as well.)

If someone says or publishes something about another person that is untrue, not otherwise privileged, and this damages the other person's reputation, this may well amount to defamation and legal consequences may follow. "online" publication of defamatory statements on Facebook, Twitter, or on blogs is still publication.

But what if the damaged reputation is self-inflicted? Although there are things that older adults may share with others in more private ways, there has never been a generation so willing to share their

innermost feelings, their outrageous opinions and their inappropriate photographs than the under-25 age group who make up the mainstay of Facebook. I hear stories about the things 15- to 18-year-olds post on Facebook through my own kids and their circle. But I see the 22- to 25-year-olds because they're at an age where they want me to hire them in my law firm. Many of these people don't seem to understand how the comments and photos they post to Facebook can be publicly accessible, profoundly inappropriate, and career-limiting.

From the 15-year-old's perspective,

...there has never been a generation so willing to share their innermost feelings,, their outrageous opinions and their inappropriate photographs than the under-25 age group who make up the mainstay of Facebook.

ive, it might be a badge of honour to post photos of her or his wayward drunken exploits on Facebook, knowing that, as their parents aren't "friends," Mom and Dad won't see last week's vodka bender. And it might be cool to tell the world you belong to groups and fan clubs that are sexually explicit, or to swear on one's wall, knowing only one's "friends" will see it.

But it's disingenuous to think one's parents (or the people close to them) won't see the inappropriate photos and comments if the teen has 750 "friends" on Facebook, (how can anyone have 750 friends?). The reality is that, despite amendments to Facebook's privacy controls to comply with the

directives of Canada's Privacy Commissioner, it's still relatively easy to see and copy what a user has posted to Facebook.

I can only echo what most of the deans of Canada's law schools tell their new students each year: "Clean up your Facebook pages. Your prospective employers are all law firms. They will be looking for you."

I can tell you first-hand, we do. All employers do. We have to.

So here are a few legal and practical things that might interest you and your students about managing and protecting their online reputations.

1. Notwithstanding new privacy settings announced in December, 2009, Facebook can retain cached archives of everything everyone puts on Facebook, even if it's deleted 60 seconds after being posted.
2. Any posting on Facebook can be saved to another's computer by a simple screen shot. And any photograph on Facebook can be dragged to another's desktop and circulated to others by e-mail, even though it may have been removed from the original poster's Facebook page. Digital pictures pulled from Facebook can be Photoshopped and otherwise manipulated in very bad ways.
3. Insurance company investigators regularly check Facebook pages of those they are investigating, sometimes posing as high school friends, or friends of friends so they can surreptitiously see the Facebook page and confirm or deny the claim. A woman in Quebec was recently denied insurance coverage when investigators saw recent pictures

of her "dancing up a storm" one night rather than convalescing at home after an apparent injury.

4. Canadian courts have ruled that one's Facebook page can be evidence and can be the subject of cross examination, even though a defendant had made his page as private as possible.
5. A court in New York City forced Google (as owner of a particular blogging website), to disclose the name of an anonymous blogger who arguably defamed a prominent model; the moral of the story being that no one is anonymous anymore. The defamed can always find the defamer.
6. Displaying your birthday and work history may be inviting scammers to apply for credit cards and otherwise steal your identity. Don't give out your birthday.

I can only echo what most of the deans of Canada's law schools tell their new students each year: "Clean up your Facebook pages. Your prospective employers are all law firms. They will be looking for you."

7. Tweets on Twitter will soon be searchable on Google, (so that tweets about how much a student hates his math teacher can be found by that math teacher).
8. Former NDP candidate Ram Lam had to abandon his candidacy during last year's BC election when the press discovered sexually provocative pictures of him on his Facebook page.
9. Users should limit the number of

friends on Facebook to real friends. If someone has 800 friends, one of them may be an insurance investigator, and another could be someone far, far worse.

10. Privacy Privacy. Facebook users should adjust their privacy settings so that only friends (and not "everyone") can see what they have posted. And never allow "friends of friends" access. Although Facebook changed its privacy settings in December 2009, the *Globe and Mail* reports that 70% of users still have their settings set to "everyone can see everything," possibly because they don't know how the privacy settings work. And of course, Google sees it all.
11. Although Facebook doesn't allow anyone under 13 to create Facebook pages, under 13's lie about their age.
12. Parents might want to monitor Facebook and other social networking activities of their teens, but teens (understandably) don't want to allow parent access as "friends." Perhaps a "designated driver" is a good idea as a friend; a young adult the teen and the parent both trust, and who won't contact parents about questionable postings or photos (but will call up the teen).
13. Finally, students shouldn't post pictures or comments they wouldn't want their mother, their grandmother, or their future employer to see, because one day soon, they will.

Tony Wilson is a Franchise and Intellectual Property Lawyer at Boughton Law Corporation in Vancouver and is an Adjunct Professor at Simon Fraser University. He has written for the Globe and Mail, Macleans Magazine and Lawyers Weekly, and is a regular columnist with Canadian Lawyer and Bartalk Magazine. His book on online Reputation Management will be published in the fall of 2010.