

The terrors of Twittering: growing up in an unexploded data minefield

LOUISA HEARN

May 5, 2010

[Comments 77](#)



Photos posted on Facebook that seem fun now may come back to haunt the subjects when they apply for credit or jobs.

Data mining is now one of the biggest minefields facing the young.

Party antics and examples of extreme behaviour posted for fun on Facebook and other social networking sites are set to become ghosts that haunt individuals when they try to get credit, homes or jobs as adults.

That's because lenders, employers and landlords are increasingly using complex data mining tools to capture all the publicly posted

data we supply to Facebook, Twitter, Flickr and any other social media network or blog to build data-rich profiles of our private lives, internet privacy experts say.



Most teenagers use social networking as their primary form of socialisation and communication. Photo: Phil Carrick

Although most of the focus has been on the marketing potential of data captured by internet data companies such as Experian and Rapleaf, few social networkers have yet considered the impact of companies using it to build a snapshot of their lives for assessing credit or insurance applications or employment prospects.

But this is exactly what some organisations are doing, according to Geordie Guy, vice-chairman of

Electronic Frontiers Australia.

"The big growth area [for data mining technology] is credit," he said.

In this context it wouldn't matter how professional your LinkedIn profile was, because pictures from the unforgettable dress-up party posted to Flickr back in 2007 might tell a bank manager or future employer a very different story.

Cyber psychologist Dr Michael Carr-Gregg said teenagers were oblivious to the relentlessly public nature of the internet and did not think twice about acting out their passions and making their mistakes online. Not only that, but they also used social networking as their primary form of socialisation and communication, he said.

Immature brains

"Their brains aren't through growing yet. The last part of the brain to develop is the frontal cortex, otherwise known as the 'voice of reason' or sober second thought. It is responsible for such things as impulse control, emotional regulation, strategic planning (anticipating the likely consequences of one's actions) – so it is absolutely understandable from a developmental psychology point of view," he said.

They are also much less discriminating when it comes to accepting "friends" online that they might not know, and unaware how easily they can be traced from photographs with identifying features such as school uniforms.

The real scandal is the lack of adult supervision and monitoring online, Carr-Greg said.

Roger Clarke, chairman of the Australian Privacy Foundation believes that as a result of their experiences online, today's teenagers will become more risk-averse and privacy-sensitive than their predecessors as a result of the negative experiences "garnered during the period of SNS [social networking service] excess around 2005-10".

But by the time enough people get burnt, it might no longer be possible to be secretive, Guy said.

"Reclaiming your online identity is like trying to unbake a cake. If potential employers have seen you drunk with your top off, you can't undo it," he said.

Social networks push for more

Part of the problem is the pressure for social networking companies to make money. Because membership of most networks is free, identifying specific audience segments becomes the most obvious way to create a revenue stream.

Even though social networks, such as [Facebook](#), have traditionally been restricted to members, the company is urging users to make ever more information about themselves public. Not only this, but Facebook has drastically changed its own privacy policies over the past few years, which means many users who think they are posting information only to their friends could in fact be broadcasting it to the entire network.

Facebook also encourages its users to keep expanding their network of friends, a move that backfired for two Queensland teachers who posted potentially [compromising](#) pictures of themselves to their Facebook network, which were subsequently picked up by a local newspaper.

Guy said that even the most clean-living internet profile can be let down by the behaviour of housemates, family or other regular associates.

"Several companies mine data to the extent that, if they trawl social networks and see you or your close associates partying too much, it might affect your credit eligibility," he said.

While internet researchers don't provide banking or credit records alongside online profiles, many of their customers already have access to this data, and there is no legal barrier to them referring to an online dossier to assess your creditworthiness.

Guy said insurance companies could also stand to gain a great deal from pattern matching your personal data on a historical basis with that of your associates.

"In the future this might affect the eligibility of your health insurance, for example, if one of your parents tweeted about smoking in the house," he said.

Supervising children can solve part of the privacy problem presented by social networking, but others outside the family can pose threats.

Photo-tags everywhere

The power to upload photographs to sites such as Flickr or Facebook, upload video footage to YouTube and tag their identity without any prior approval has become universal and, with photo-tagging technology now spreading beyond Facebook to the wider web, content is becoming increasingly searchable, Clarke said.

"It has become a norm to apply informal tags to image and video, with the result that many non-text objects are also subject to searching," he says.

While those in trusted professions such as teachers and policemen must pay particular attention to what they place in the public sphere, even more vulnerable are children and teenagers, internet experts say.

For many, the overriding concern when it comes to sharing private details online is impressing their peers, and finding an outlet for troubling emotions.

Photographs from parties and even the school yard are prime candidates to become permanently associated with their online profile and, once this type of data appears online, it becomes almost impossible to remove, said Alistair McGibbon, managing partner of Surete Group, an internet security consultancy.

"By the time it has proliferated, it spreads exponentially. The reality is that it can never go away. What you need to do and hope for is that time will bury these things.

"I think there will be a loosening of social standards so that people are less upset by what they see," he said.

He added that there were some benefits to a more transparent society. "People were once able to move from location to location and conduct business that was improper. It has helped in reducing some of the shyness out there," he said.

But what happens when that transparency goes too far. Guy said that location-based technologies take the argument beyond privacy and into the realm of personal safety.

Location-sharing networks such as Foursquare – which recently celebrated its 1 millionth customer – are becoming increasingly popular among youths who like to broadcast their movements to friends.

"If two social networking sites hook into each other, you can find you are giving away a lot more than just the sum of info contained in them both. If you look at Twitter and Foursquare together – if they are integrated and you are providing information simultaneously, you can be telling people where you are, who you are with and what you are doing. People may not be doing the sums in their head to realise what they are putting out there," Guy said.

McGibbon agrees that publicising your location opens up a whole new arena of risk.

"I have turned off the geo-tagging functions on various services I use. I am just not ready to be that exposed," he said.

How to stay private

- Do not permit children or young teens to use Facebook unsupervised. Set clear usage limits and

educate older teens about the dangers (present and future) of "oversharing" online.

- Be cautious about what you write and the pictures you post. Ask yourself how these might be viewed in years to come by someone you want to impress such as a boss or bank manager.
- Avoid posting birthdates or including children's names in photo captions or tags.
- Create a pseudonym and private email account for contributing to forums where you want to give your opinion or feedback in a private capacity.
- Sift through all of your privacy settings on applications to ensure you are only sharing photos, videos and other very personal data with people that you want to, and stay up to date with any privacy changes the application makes to these as time goes by.
- Remove any identifying "tags" from photographs or videos posted by friends of you or your family that you don't want others to be able to access now or in the future.
- Restrict your friends' lists on social networks to those you actually know - or reclassify them into different groups, each with their own appropriate privacy settings. Double-check the profile of new contacts or friends asking to join your network.
- Remove any activities, interests and regional data from your profiles that you don't want people outside your network to know.
- Think twice about broadcasting personal details or images that might identify your location or future movements.
- Use strong passwords for accounts to prevent them from being compromised, and switch off the option for your account to be found via a search engine.

Source: smh.com.au

Comments

77 comments

»«

*»Facebook has been 'Stalkbook' since day 1 of its operations began.
I set a page up just so a stalker that was miffed with me for dobbing in him into authorities (using South Korea's better defined net stalking laws/digital privacy laws) couldn't create a fake facebook page in my name and then write hate posts (which is something cunning netanimals do) etc.*

He came after me and got me in other ways anyway- he tracked me by googling my email and then finding my ip number which he then further tracked backwards etc... he then got the name of a friend etc and then my mobile number.«

»# Another particularly bad method data miners use is placing fake adverts on job websites. We then send highly detailed resumes to them.«

»«

Alex | Finley NSW - May 05, 2010, 1:47PM

»«

»What also worries me is that organisations even think that photos of people when they were teenagers is even relevant to a job application or for credit. Or even recent photos of a night out. I know plenty of people who go out and have a few drinks or yes, even go to a dress-up party, but that has nothing to do with their ability to do their job during the week.«

»It might say something about their judgement that they've put things up there in the first place but I think this kind of info should be kept as private as possible because it's largely irrelevant.«

»«

Biffsteak | Sydney - May 05, 2010, 1:45PM

»«

»When Facebook first appeared my first thought was why would anyone want to use their real name on the Internet.«

»Beggars belief.«

»«

Adrian (not my real name!) | Adelaide - May 05, 2010, 1:33PM

»«

»and lastly, make sure when you tweet you don't work for a major media company which doesn't respect free speech.«

»«

thaddeus | stanmore - May 05, 2010, 1:51PM

»«

»There's not a day I wake up with being thankful I'm not on Facebook, Twitter, MySpace etc etc.«

»Selling everyone's info is a revenue stream that can't be ignored.«

»«

sydneyner - May 05, 2010, 1:55PM

»«

»Of course, all you need to do to erase your past is change your name. Even changing one or two letters will create havoc in those mindlessly trying to dig up dirt. Once you're married, it's a whole new ball game.«

»«

JayneM | Sydney - May 05, 2010, 1:54PM

»«

»Parents are way too lazy to supervise children using facebook. Most have no idea what goes on and are happy to keep it that way.«

»«

Williamu | Wollongong - May 05, 2010, 2:06PM

»«

»The hardest thing is to delete friends from Facebook when they go astray or become offensive«

»«

K.B. - May 05, 2010, 2:06PM

»«

»Just don't join a social networking site.....ever!«

»«

eyeroll | Sydney - May 05, 2010, 2:05PM

»«

»Biffsteak, I was recruiting for a job last year, and I can assure you I checked the names of all of the candidates on all of the social networking sites. Someone who has photos of themselves partying every weekend is not someone who is going to be a reliable employee. How many "sickies" are they going to pull because they're hungover? I binned every single candidate who looked like a party animal, or who had made racist/sexist/homophobic/etc comments on those sites. Why would I want someone working with me who is an intolerant moron?«

»«

Jen | Brisbane - May 05, 2010, 2:14PM

[Show more comments](#)

Comments are now closed

»“Reclaiming your online identity is like trying to unbake a cake. If potential employers have seen you drunk with your top off, you can't undo it.” «

Top Technology articles

1. [Facebook users urged to quit amid privacy concerns](#)
2. [Warning: Facebook malware attack on the loose](#)
3. [Internet addicts guilty of starving baby to death](#)
4. [Calls for internet access to be enshrined as a fundamental right](#)

5. [Now Bangladesh blocks Facebook over Mohammed](#)
6. [More Technology articles](#)

Latest Comment

» *Jen X - May 05, 2010, 3:14PM*hahaha love it. australia at it's best «
poor banker
[See comments \(77\)](#)