

# Get out of my face book



## There are clearly identifiable risks involved in cyber networking but simple precautions are available to avoid them

WHEN WILL SOCIAL networking sites cease to be cool? Millions of us who thought that signing up to these would gain us access to a world of ever-growing friendships, socializing, and fun without consequences may now be learning otherwise. But could it be too late?

According to Roger Clarke at the Australian Privacy Foundation, the bad experiences many online teenagers have suffered will mean they'll be less inclined to take risks and seek greater privacy in future as a result of the excesses of social networking.

But in many cases the damage has already been done. As vice chairman of Electronic Frontiers Geordie Guy related to the

Australian Herald: "Reclaiming your online identity is like trying to unbake a cake."

Clearly the young are at greatest risk of using social networking in an irresponsible way that can lead to unpleasant circumstances, from peer ridicule to bullying and even the greatest fear of all – grooming by a predatory adult. This is because they've yet to develop the neurological hardware in the front of their brain that will eventually tell them: "What I'm doing isn't smart, there could be consequences." Instead they act out their passions on a vast public stage they're only nominally aware of.

But even if we're all grown ups here, many of us are only partially aware of just how much of the information we think we're only sharing with "friends" is in fact up for grabs by people we don't know. And the risks are increasing.

At one level, social networking sites are constantly urging us to give up more of our personal information. The temptation is often to click away our rights just to stop the distraction of these requests and get back to networking. If we come unstuck and receive unwanted attention, this is clearly our own fault. But at a more insidious level, some social networking sites have drastically changed their own privacy policies since inception. This means many of us who think we're posting information exclusively to our friends could in fact be broadcasting it to the entire network.

The consequences of so much of our private information swirling around in cyberspace can, at one extreme be fairly benign if irritating. Sites like Facebook and other social networking sites are manna from heaven for marketers as all the information we give away so freely makes it easy for advertisers to target audiences like us. But these are not the only eyes that could be on us.

## FUTURE PROSPECTS

Whether we like it or not, updating our profiles on social networking sites could amount to an inadvertent addendum to a CV for a potential employer or a black mark on our credit rating.

According to Mr Guy, data mining technology is gaining a new lease of life with an avid interest in credit. In this context it matters little how you present yourselves to others within your professional existence, a photo posted of you, on one of your not so good nights, will paint a different picture to owners of a possible credit line in the future.

And when it comes to employers, Maxine Frances Roper wrote to the Guardian in March this year that, "the practice of employers running internet searches on employees is now so widespread that employment agencies offer advice on online reputation management."

And there are also the unknowns. As we exchange information, how many of us are actively thinking who's logging this data? Who's controlling it? And who wants it? Can I remove it? Is it being archived? If you think you can find out the answers to these questions now – and it's doubtful – consider the future. Social networking sites are the hottest cyber tool on the planet right now but what if other companies with less than upright credentials buy them?

It seems unlikely at this point in time, but if social networking is eventually found to be un-cool, what will become of their assets? Don't forget those assets are you.

Another unknown is perhaps the hardest one to deal with. In the unlikely event that you're not a user of social networking, you could

**“Clearly the young are at the greatest risk of using social networking in an irresponsible way that can lead to unpleasant circumstances”**





still be in the firing line as your friends are probably putting you online by proxy, simply by tagging you in a photograph. Would you feel comfortable asking friends to remove pictures of you from their account?

The ability to upload photos and video footage to sites like Facebook and tag the identity without prior approval has become universal. With the technology now available to move this content to the web, content is much easier to search. Once such images have leapt over the almost non-existent barrier between someone's account and the wider web, it will simply spread and spread and never go away.

## TRACKING ME TRACKING YOU

If you're not scared into taking more care about what you disclose yet, take note of how easy it has become to take the leap from concerns about personal privacy to fears about personal safety. Location based technologies add a whole new dimension to the potential consequences of releasing personal information.

Many people like to broadcast their movements and by two social networking sights hooking into each other, the sum of the information is - who you are, whom you're meeting and where you are. What more could be needed by people you surely don't need to know? Publicising your location creates a whole new area of risk.

In reality social networking should be a fun extension to our more face-to-face socializing but it's worth remembering to take some precautions.

## STAY PRIVATE

If you permit your children to use networking sites do supervise their usage and set clear limits to their time online for their benefit and yours:

- f** If you permit your children to use networking sites, supervise their usage and set clear limits to their time online - for their benefit and yours.
- f** Don't post birthdates or include the names of your children or others on your photo captions and tags.
- f** Think before you write and post pictures: is this what I'd want others to see or read in the future?
- f** If you want to contribute your ideas to a forum in private, create an email account with a pseudonym.
- f** Always check your privacy settings on applications to make certain that you're only sharing videos, photos and other private data with people you want. You should revert to privacy settings frequently as changes may be made to the application at any time.
- f** Avoid the temptation to accede to friend requests from people you're unfamiliar with and double-check the profile of new contacts and friends requesting to join your network.
- f** Take care to remove tags from photos or videos posted by your friends, of you or your family, which you wouldn't want others to see.
- f** Beware of advertising personal details or images that might identify your location or future movements.
- f** Finally, think of strong passwords for your accounts to ensure they're not compromised, and switch off the option that allows your account to be traced through a search engine.