Best Feature in IT Journalism

JAMSHED AWARI

BEST FEATURE IN IT JOURNALISM

Jamshed Awari won the PoleStar Award for 2010 for his article, 'Safe Social Networking', which appeared in CHIP, dated February 2010.

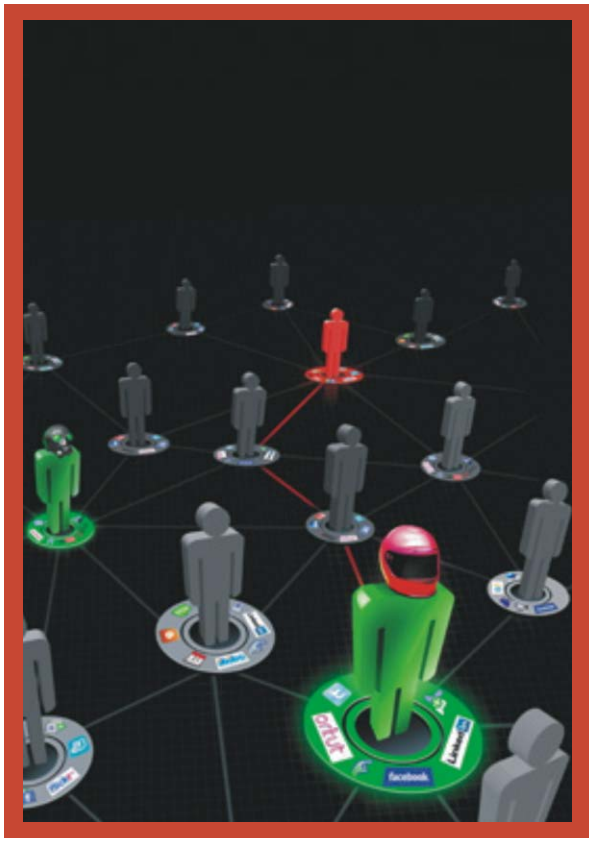
Jamshed Avari has been working with CHIP for around five years as Deputy Editor and plays an important role in managing the content and work-flow for the magazine each month, as well as strategic planning, editorial marketing, and industry relationship activities. Previously, he was a part-time writer and reviewer for CHIP apart from a few other publications and websites while completing a post-graduate diploma in New Media and Journalism, and a bachelor's degree in Mass Media (Advertising).

Safe Social Networking

Jamshed Awari

February 2010

You're connected to more people than you know, and that innocent photo of last night's party could harm you in ways you never imagined



One day, out shopping, you meet a long-lost school chum. You chat, exchange news of common friends, share a few laughs about good times. You part, exchanging phone numbers, even joyously arranging a get-together at a future date. But you probably don't rattle off details of every place you've been and every friend you've made in the last decade.

Imagine now that instead of bumping into that friend in the mall, you chanced upon his Facebook profile, and sent him a message and an invitation. Unless you're the paranoid type who keeps your online privacy levels high, you've just handed him a summary of the activities of your life, plus access to your photos and videos, personal thoughts, group memberships, and list of other friends. All this despite not knowing the first thing about what he's been up to and the company he keeps.

A few days later, you see you have friend requests from a dozen other former classmates, none of whom you were particularly good friends with or would consider contacting yourself; they saw your name pop up in their news feeds, you see. You feel awkward about ignoring them… so you click 'Accept.' Each one of them can now see every last detail about your life. That one encounter spawns a dozen more, and each could spawn another dozen. Very quickly, your online connections grow into a vast, overlapping, network of interconnected strands. And you lose control over not only who you're connected to, but who can steal your information.

Your photos could be copied, altered and reposted online. Your email address could be harvested by spammers. Your boss could frown on evidence of your carousing. Your co-workers could shun you for things that are none of their business. Your parents could mortify you by leaving comments on your friends' updates!

Welcome to the Network

MySpace, Facebook, Twitter, Hi5, Orkut, and dozens of other mainstream or niche social networks used to be vast, open playgrounds where people freely posted about the most intimate details of their lives. Today, that is a bad idea.

There are a few major causes of concern. That enormous corporations are building detailed databases and distilling your profile information into marketable slices is dangerous, but abstract; you don't worry about it that much because you can't see it happening and you probably wouldn't be able to identify an incident that has disrupted your life as a result.

But information about you can be seen by strangers, your updates can reveal your movements to undesirable people, and you expose yourself to a huge amount of liability even with family and coworkers.

Take stalkers. A twenty-three year old from Mumbai, who prefers to remain unnamed, got repeated friendship requests over the course of several months. She didn't know who the person was — his profile had a film star's photo and (misspelled) name, and no friends in common — and kept declining. The requests began including references to places she

had recently visited, and at least one vulgar comment about her partying and drinking. Frantically checking her security settings to make sure her updates weren't visible to strangers, she realised that photos tagged with her name were visible not just to friends, but also to strangers tagged in the same photos and their friends; she had absolutely no idea how many people could see them and who they were. She eventually used Facebook's flag feature to report abuse, but still has no clue whether the stranger was someone she'd met, or who might someday accost her.

(Note: Indian police cybercrime cells are actively involved in tracking down such stalkers; approach them if you ever face a similar situation.)

Another example: Aashish, fresh out of college and settling in at his first traineeship with a financial consultancy. A week or so in, one of his superiors made a remark about how he'd seen stress lead to drug use in extreme cases and that young people today seem to not be scared of drugs, all the while looking pointedly at him. He thought it was odd but dismissed the incident. Months later, he found out that his boss had seen printouts of a string of comments left on his Orkut profile by college mates making jokes about being inebriated. The company's HR had made it a practice to check out, in the most common social networks, the names on all resumes they processed, presumably as a form of background check. It hadn't cost him the job, but it had certainly coloured his colleagues' minds even before he'd had the chance to make a first impression.

If you think the volume of information about you readily available to strangers is staggering, the situation is getting worse.

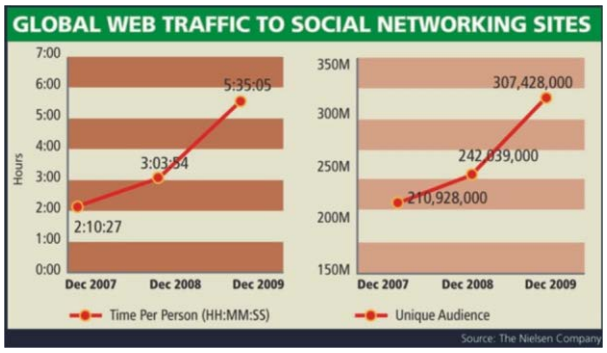
Twitter will soon start a broad rollout of location-aware services tied to timelines of user activity. This will let you discover interesting users in the vicinity, but will also allow your coordinates to be mashed in, telling the world not only what you're doing, but where you're doing it. If you're using a recent smartphone, chances are your coordinates have been transmitted with your Tweets for a while already, but haven't been displayed publicly. Facebook is likely to emulate this any time now.

Where Does All the Info Go?

One word: Advertising. Facebook serves ads to its users based on activity and relevance. Orkut data gets fed into the enormous mines of information that Google already has about its users.

The good news? Most sites have been hounded about privacy enough that they have clearly stated policies about what data is retained, and what kind of metrics are shared with third parties.

Facebook was at the centre of controversy last year when it emerged that advertisers could use members' profile photos in ads, to demonstrate that a person's friends were already users of the product being advertised. Facebook officially termed this



"abuse" and went on to ban others from doing this.

The lesson: Get well acquainted with your privacy page. And note that external applications, including your own mobile phone and other sites which let you sign in to update your profile, will have their own privacy policies and settings, some less benign than others.

Then there's real-time search. Bing and Google News users might have noticed Twitter posts popping up in their search results, auto-refreshed even as the results page lies open. Live status updates are the latest search frontier; everyone wants in. Social networks will partner with more and more search engines in order to be more relevant.

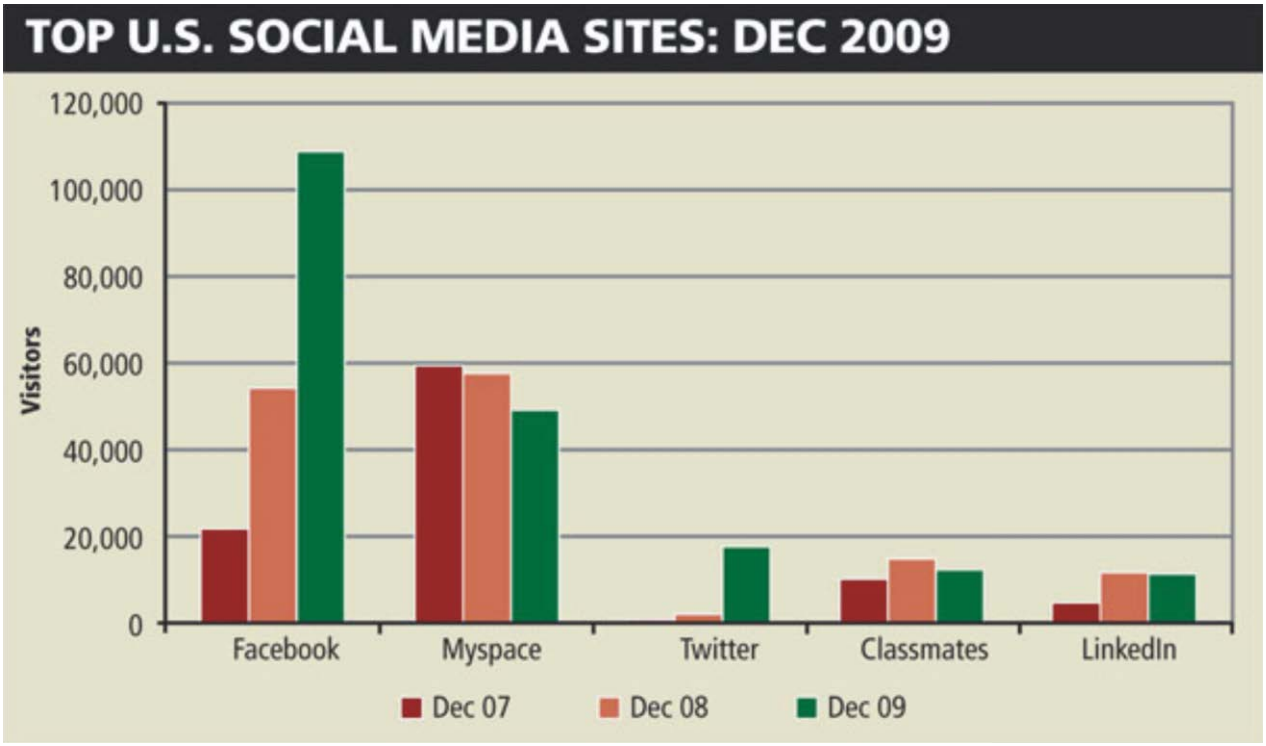
Social applications — games, those silly quizzes — also have a field day with your information. When you use a third-party app, you authorise it to access profile information — location, date of birth, and friends list — which is then used to spam your friends with messages aimed at bringing them into the fold as well.

Unethical apps prompt users to either divulge more information — which is then outside the scope of any host network's privacy policy — or pay money using real-world credit cards in order to advance to a higher level. Applications have already been banned because of this, but the amount of money coming in is hard to ignore.

Striking a Balance

Remember this: It's perfectly okay to decline a friend request. Better safe than sorry; and there are ways to deal with those who might be offended. Get familiar with your networks' security settings. Set privacy levels, and keep checking to make sure policies haven't been altered by the site — it happens quite often.

Set up groups or lists of friends. The exact terminology varies by network, but the controls can usually be found under Security or Privacy settings. Lists allow you to define access privileges for everyone in them. If you absolutely cannot decline a request but don't want the person in question to see every last detail in your life, put the person in a list whose members can see only minimal information. You can group people by the distance you want to maintain: Co-workers, acquaintances, old friends, family, relatives, etcetera.



Remember, opening up any part of your profile to "Everyone" also makes it visible to search engines, which means, basically, anyone in the world can see them. Note: on Facebook, "Everyone" is now the default setting for many parts of your profile. But there's also a handy default "Restricted Profile" list, where you can add people to your friends list while keeping them blind to your activities and interactions. And while creating a photo gallery, or even a single status update, Facebook now lets you choose which sets of people should be able to see it, over and above the default rules you create in the security settings. Of course you'll need to keep track of who is in which group and change things as relationships change.

Comb through your settings thoroughly. You'll find options for sharing your behaviour tracks with third parties, or publishing information about your activities. Check all Facebook applications thoroughly, especially the free games!

The simple fact is that every added security measure makes the sites less appealing. You alone can decide how much of your life is open to the general public. Remember, no one's a stranger. Things you post online can come back to bite you years down the line.