SWCP PORTAL

Providing News, Views, & Clues from Your Local Internet Experts 201009

Life in the global village

Who’s Watching You?

By Jay Nelson, editor

Some scientists believe that the uncanny feeling people often get when they’re being watched is occasionally an accurate extrasensory perception. If so, it would be understandable if Internet users find themselves a bit twitchy and vaguely uneasy these days, for they are now being tracked online more avidly than ever before. It’s only going to get worse, so get used to it.

Of course, there’s no real dividing line between Internet security concerns and privacy issues. One fades into the other. But privacy is a broader, more diffuse concept which can complicate the most innocent and enjoyable online activities in unexpected ways.

It is often those very sites that freely offer the most valuable services which gather the most data on their users. For the old proverbs remain true even in the Information Age: “there’s no such thing as a free lunch”, and “you get what you pay for”. If you’re not paying cash online, you’re likely paying in **data** — about you, your browsing habits, spending, social connections. It’s all done in the name of making things easier and more convenient. The question is *for whom*.

There’s no doubt that many of these innovations are of genuine benefit to users. But such technologies developed with the best intentions can be misused or have unintended results, too. For instance, social networking sites like **Facebook** and **Twitter** are experimenting with geographical location features, under the reasonable assumption that knowing your friends are nearby would make it easier and more fun to connect with them.

Yet already there have been several burglaries reported and social fiascos that were made possible by thoughtless “social oversharing”. For one thing, you can tag the friends you’re with. There is also the question of what happens to the “little white lie”. Scorned by moralists and moms everywhere, these fibs actually perform a valuable service. They allow people to gracefully avoid unwanted situations without causing undue offense.

The “**right to privacy**” is just one of the countless social assumptions that have been carried over into the virtual world from the real one. But the problem is that these hardwired metaphors do *not* adequately describe the true capabilities and behavior of this brave new world we now inhabit. Our expectations have not managed to keep pace with the technology; a brand-new set of social rules must be developed to deal with it.

Most people regard email as old-time postal letters, sealed in an envelope, contents snugly hidden and protected by law, in real world terms are really nothing more than electronic postcards. *Anybody* from the mail carrier to random visitors can read them. Likewise, your Facebook page is just a bulletin board in the middle of Times Square — one of half a billion, but still instantly discoverable by anyone who cares. But the one to whom it matters the most, naturally, is Facebook.

In fact, both twin giants of the Internet can track you most places online. You may have noticed Google ads following you around the Net. And even if you thoroughly avoid Facebook, the social networking colossus probably already has a file on you. Whenever someone new joins who wants to “friend” you, you get an email that lists him or her, plus anybody else who has ever asked to friend you — and a bunch of other people Facebook thinks you might know, besides. Evidence suggests that even if you quit, your account may be deleted, but *not* your data. It seems that no-one can truly escape.

Not long ago, with all the bad publicity about users being stalked and harassed, even driven to commit suicide, and to protect teens and children, the site has taken steps to improve privacy. Facebook has placed alert buttons to mark inappropriate content. The website announced new privacy settings that allow members to customize who gets to see updates, specifically or for all of them. Kids and workers, it seems, were unhappy that parents and bosses could so easily follow them.

However, the site also recently launched a new feature, a button on affiliated webpages that members can click on to announce they “like” the content. This gives the user a chance to share enthusiasms with others, and provides a gold mine of personal data for advertisers — what Facebook’s rival Google calls the “crown jewels”.

Continued on back

Never lose homework with the SWCP *SchoolBUS*

Kids can be their most creative when coming up with reasons for not having their assignments. In the Internet age, according to some British teachers, modern common excuses range from "I left it at home" or "the dog ate my flash drive" to the "printer was broken" and their favorite; "Russians hacked my dad's computer".

Now, with SWCP's new SchoolBUS Online Lockers, it will be harder for students to get away with such tall tales, and easier on parents. Like our regular BUS backup service, the SchoolBUS automatically uploads copies of digital files from their laptop or PC to a secure server every night over their own broadband connection. There the data remains safe but accessible from any Web browser. Old copies and changes are stored, too, so there's no danger of accidental deletion.

SchoolBUS offers more than a semester (6 months) of backups for only $**30**. With 5GB of space, the locker should be big enough to hold everything but their lunches. Intended specifically for students, a current acadmenic ID is required, but there's **no signup fee**. So call today, and sleep better all school year long.

Net Notes

Supersize Your Passwords for Security

According to CNN, researchers at Georgia Institute of Technology have shown how much more secure longer passwords are than short ones. Using a stack of graphics cards, they were able to crack 8-character passwords in a mere 2 hours using a trillion combinations per second. Calculations indicate that using 11 characters would increase that time to 180 years, while adding just one more than that means that it would take an astonishing 17,134 years to crack.

Passwords have steadily grown over time: now the experts recommend **12 characters or more**. Start with an entire phrase or sentence, such as "I like both red and green." Take the first letters and make an acronym, replace some with similar-looking numbers (like "1" for "l", "0" for "o"), mix lower and upper cases, throw in some random symbols, and voila! A unique, uncrackable but memorable password.

SWCP allows 8-15 character passwords, and suggests that they be changed every 3-6 months. You can easily do so yourself at "**Member Tools**" on our website.

Continued from front

Google has not avoided criticism, either. Their mapping program's "Street View" option, which gives users a ground-level view of the actual location has gotten them into serious trouble. In Great Britain, which has one of the highest concentration of street surveillance cameras in the world yet every man's home remains his castle, the pictures were thought by many to be an uninvited intrusion. And indeed, Street Views have allowed people who claimed to have stopped smoking to be spotted sneaking cigarettes outside, not to mention busting others coming out of various seedy establishments.

But all that was nothing compared to the uproar that grew out of recent revelations that Google was "accidentally" logging wireless data during its drive-bys — over 600 GB in more than 30 countries. Despite the fact that the data was being broadcast unencrypted and thus freely available, suspicions erupted over what purpose the company wanted it for. European nations and even India began demanding to know; and governmental demand for access has spread to other services, such as Blackberry's encrypted email and Skype's phone service.

The heads of both Google and Facebook have been trashed for their secretive attitudes as to the proprietary uses made of data collected. In fact, an "anti-Google" campaign has just been launched by the Consumer Watchdog privacy advocacy group (*insidegoogle.com*) with ads in Times Square after Google founder Eric Schmidt made some ill-considered remarks. "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place," he said.

He didn't win any points either when he later mused that children should be allowed to easily change their names when they grow up to escape any embarrassment from youthful indiscretions in their online lives. Commenters quickly pointed out that his own search engine could just as easily discover name changes as anything else about a person, so that wouldn't work at all.

Consumer Watchdog president Jaimie Court said that "Google knows more about us than the government does," and that "Schmidt is out of control." However, despite the cavalier attitude displayed, the man has a point. Schmidt is quite correct in his basic, if unspoken, assumption that the world is now **one global village**.

The Internet began as a tiny community, a network strung among a few mainframe computers and university researchers. They all knew each other, and thus it was easy to police behavior. So the methods they designed were too idealistically user-friendly and trusting.

With the birth of the Web, the fantastic growth that resulted destroyed much of that sense of community. But the Internet remains the biggest small town *ever*, with all the pluses and minuses that kind of forced closeness implies. We're all going to have to figure out new ways of getting along, living together in cyberspace.

So while their elders continue to fuss that someday they'll be sorry, the younger generation posts on, blissfully unworried about who sees what. Time will tell, but so far, it seems that the kids are all right.