SWCP PORTAL
Providing News, Views, & Clues from Your Local Internet Experts 201003

WWW Newswatch

Online Privacy Update

By Jay Nelson, Editor

There seems to be both too little and too much privacy on the Internet these days. While hackers and scammers manage to wreak havoc while lurking anonymously, many honest, normal people are finding their personal data vulnerable and exposed to criminal uses.

Technology itself may be neutral, but it's developing so uncontrollably fast that it seems like a new threat or twist is revealed every day. Here's a round-up of some recent headlines, illustrating how these issues already affect all levels of society, from international politics down to home and school.

Big, bad hack attacks

In January, search engine giant **Google** announced that it might be ending its controversial cooperation with China after being hit by a coordinated series of hacks. The hackers had apparently stolen intellectual property and attempted to access the Gmail accounts of hundreds of Chinese human rights activists.

The attack was described as highly sophisticated, using a dozen malware programs and levels of encryption to avoid detection. Not only that, but at least 33 other major companies, including Adobe, other software and some financial institutions, were targeted.

The hack involved an email with an **infected PDF** document that used a newly-discovered vulnerability in Adobe's Acrobat Reader. Patches have been hastily devised to cover the security gap.

Another operation going on since 2008 from Eastern Europe has allegedly broken into more than 75,000 systems at nearly 2,500 companies worldwide. Like the Google attack, it was also based on luring unsuspecting workers at targeted firms to open infected attachments.

Perhaps coincidentally, the **NSA**, which Google asked for help, recently wargamed a cyber-attack scenario. The results show that Net security has a long way to go yet, and many legal tools need serious upgrading.

FTC v. P2P

Security breaches don't always come from the outside, either. The Federal Trade Commision recently notified over 100 unidentified companies, schools, and local governments, of data leaks from within involving the personal information of employees and customers.

The FTC said that sensitive data, useful for identity theft, had been uploaded from the internal systems of the companies by **peer-to-peer file-sharing** networks, where it was freely available to any user. Enterprises ranging from small shops to large corporations are equally vulnerable. The government urged all institutions to review security policies, and make sure that there is no unauthorized P2P file-sharing going on.

Webcam gamboling

Online **social networking** presents a whole slew of new privacy concerns. One site, only three months old, has already had warnings to parents about it issued by child safety advocates and places like CBS News. Aptly named *chatroulette.com*, the website randomly connects people with live webcam feeds.

While no information is exchanged unless one wants to and a single click is all it takes to move on, the site, meant for those over 16, is otherwise unregulated for age or content. Apparently groups of teens get together to surf and share their reactions. And according to reports, there's plenty to go "Ewww!" about.

Child safety advocates say that this is yet another reason to keep Web-enabled computers only in the public areas of the house, and *never* allowed in the kids' bedrooms.

Another site under the scrutiny of CBS's big eye is one supposedly set up specifically to warn users about the "potential reach" of social networking media. Called *pleaserobme.com*, it's a location-sharing website that collects and reposts Twitter and Facebook messages that tell where people are when not at home. While praised for good intentions, it has been sharply criticized for actually giving the bad guys invitations and assistance.

The buzz about Buzz

Google itself came under criticism for exposure of possibly sensitive information. Its new service, **Google Buzz**, is for Gmail users wanting social networking services like Twitter or Facebook. But users were automatically signed up, follower lists generated from email address books and chat contacts, along with shared items from Picasa photo albums and Google Reader — and then they were all publicly displayed.

Due to the instant uproar, Google quickly backpedalled, removed the auto-signup and allowed the fol-

Continued on back

Continued from front

lower list to be hidden or the service disabled. In reality, their actions weren't too different from Twitter, except that Twitter is a well-known social networking site, and Gmail is an email service where privacy is expected.

School spying

Google clearly didn't think the situation through but claimed that they meant no harm. This is also the excuse of the Lower Merion School District in eastern Pennsylvania for spying on its own students via webcams, but it might not spare school administrators any grief.

Laptops with built-in webcams were issued to the schools' students. The cameras could — and were — turned on by administrators remotely, without students' awareness or permission, in the privacy of their homes. Officials claimed it was to recover stolen computers, though none had been and there are much better ways.

According to spokesmen from the ACLU and the EFF, such action by *any* government agency, including a public school, would be illegal, even if known and consented to by parents. Other forms of monitoring, including key-logging, screencaps, and web-tracking are also likewise forbidden. Yet, federal wiretap statutes would *only* apply if the school actually listened in — the antiquated law covers audio communications, but not video.

A lawsuit has been filed, and the FBI is investigating the case. Folks worried about such potential spying may cover the camera with a sticky note to defeat video surveillance, but there's no switch on laptops yet to turn off the microphone. Obviously, it's not just the government that has some distance to go to prepare for the intensely-connected world we all now share.

Net Notes

The Cookie Jar

Web users have been warned for years about the security issues involved in "**cookies**" — tiny files placed on your computer by websites you visit. While they can be quite helpful to you by tracking your surfing preferences and return visits, cookies are also one of the main methods advertising firms like Google use. With cookies' help, such companies build up huge profiles of users over years and years of tracking them all across the Web, in order to target their advertising much more personally and effectively.

But the old advice about limiting cookies and regularly deleting them is insufficient. At least 5 other cookie-like tracking methods are now used which browsers do *not* regulate. One of the most common, the "Flash cookie", is maintained by the Adobe Flash plug-in for use on pages with embedded applications. Users not only lack control over these "**supercookies**", they never expire, and may even be used by websites to restore their previously-deleted Web cookies!

Cookies may be shared with third parties. Social networking sites use them to pass names, profiles, lists of friends and other information. By such means, many websites, including some of the largest and most popular, manage to circumvent users' privacy preferences.

— EFF

Ebooks and readers' rights

Reader Beware

By Jay Nelson, Editor

Whether read on a smartphone, a tablet, a netbook, laptop, or desktop, electronic books are the coming thing. But, as mentioned last month, there are a lot of questions about rights that have yet to be settled. However, just as in the contests between video formats, consumers still have a chance to influence the outcome by the choices they make and the features they demand.

Here are some questions that the Electronic Frontier Foundation (EFF) thinks readers should take into consideration *before* purchasing a digital book or ereader.

Does your ebook reader/service protect your privacy?

Private reading is essential to freedom of thought. Ebook usage — even the individual pages viewed — can be tracked much more easily than that of paper. The EFF opposes user registration and logging.

Does it tell you what it's doing?

Stored account and other information should not be disclosed about readers' choices without court order and reader notification. Both a commitment to transparency and enforceability of reader privacy should be required of all ebook publishers.

What happens to any additions you make, including highlights and commentary?

Paper books are easy to mark up with all kinds of notes, dog-earred pages, or bookmarks. Sometimes the annotations can make it a whole new work. Is it possible to do this to your ebooks, and if so, what happens to the notes and who controls them?

Do you actually own the ebook, or just license it?

This is perhaps the *key issue. Purchasers of physical books can do anything they like with them, including giving them away, reselling them, throwing them out or keeping them forever. Or they can be borrowed for a limited time from a library. Which way does your service work? With ebooks there is also the question of format, and which physical platform and/or ereader software can open them.*

Is it censorship-resistant?

Without protection, ebook publishers could become censors with power beyond Orwell's worst nightmare. Already Amazon has deleted purchased copies of **1984** *from users' Kindles in a copyright dispute! Countries where the services reside might also exert undue influence, as might other large corporations.*

Is it burdened by DIgital Rights Management (DRM)?

Already being used by Kindle and other early entrants, DRM limits what you can do with the copies you buy, usually to prevent copyright infringement. But as the experience of the music industry shows, DRM curtails consumer choices, may open security vulnerabilities on computers, and takes away the power of authors to control their work. Worse, it is completely ineffective at preventing copying — a camera, an Optical Character Reader and some determination are all that is needed to defeat any such ebook "security".