Crossing the Digital Divide (v108)
"Lookout!"
by Joseph Feigon
for the Observer

Scott McNealy is an American businessman. He is most famous for co-founding the computer technology company Sun Microsystems in 1982 along with Vinod Khosla, Bill Joy and Andy Bechtolsheim. Oracle Corporation (Larry Ellison's database client) purchased Sun Microsystems in 2010.

Mr. McNealy was one of the relative success stories in the early days of the Internet. Sun Microsystems built exceptional servers, and was a market leader with their Unix operating system as well as their corporate support of the Open Source movement, including Linux. Sun 'cuda been' a contender.

Lookout was McNealy's inverted name for Outlook, Microsoft's e-mail client.
McNealy says you need to "look out" for trouble when using Outlook. McNealy frequently cites Outlook's well documented security problems. He says that to get the most functionality out of Outlook you'll also need Microsoft's Exchange Server. But the combination, and the Microsoft-only mail and calendaring protocol required to connect them (MAPI), is yet another example of how Microsoft locks businesses into proprietary technologies that eliminate choice and flexibility.

Microsoft is still here, Sun Microsystems is not. Proprietary software continues to dominate the retail customer (Windows, anyone?), as well as many big companies. Those success stories in the Open Source space build applications on an Operating System (Linux, BSD, NetBSD, FreeBSD, etc.) that is open, meaning, free to you and me. Open, as in, anyone with the desire and/or ability can review each line of coding that makes things work. Hard to hide information that way.

While we're on the subject of control, let's take a step back and talk about you : who has your data, how much do they have, what are they doing to protect it (you), and how can you improve their job.

90% of the email users in this country have a FREE account with Google. Gmail is free, Gmail is powerful, Google manages security far better than the likes of Equifax, but as we learned recently with Facebook, what goes in can come out. Yahoo also offers free email, alas, we know how secure they are. Outlook (Microsoft) is the new name for Hotmail. Microsoft is still Microsoft.

None of the big "free" email account providers are without ad support.

This weeks' take-away is two part, both designed to keep your digital profile minimized, both a means by which you can opt-in where and when you want.

1) Quit using Google for your searches. Google provides a "free" service in exchange for tracking your Internet activity using cookies. Let's say I do a search for hot water heaters – the results will yield the obvious (Lowes, HomeDepot, Sears, etc.),

companies that pay prime dollar for ad placements, followed by local (or not) product/service providers. The next time you open your browser to search, you will be presented with ads for water heaters. Cookies are often viewed as malware, as they keep Google (and others) apprised of your viewing activity. No fun, right?

Instead of Google, try duckduckgo.com, an organization that feels as strongly as many of us do about being watched, our activity tracked, and our choices sold.

By-the-way, if you find something “free” that works for you (like OpenOffice, LibreOffice, Thunderbird, Wikipedia, etc.) consider making a donation via Paypal.

If you really want to live without Google, try Firefox or Opera as your browser instead of Chrome.

2) Use encrypted email for secure, end-to-end communication.

Email isn’t secure. Email is a plain text application. Whether you use webmail, Thunderbird, Macmail, Seamonkey, Mutt, K-9 mail, Eudora, Outlook, the contents of your email *can* be viewed by anyone in the chain of delivery (including your ISP, including the ISP your ISP uses, including the govmint). Nothing is private unless it’s encrypted.

If this sounds too geeky, it need not be. Check out protonmail.com, a Swiss based company who provides personal and business email encryption service, end-to-end. End-to-end encryption means no one can read/intercept your mail in the middle and actually read content. Email then can’t be read.

Cookies are trackers, software designed to feed information about your activity online to those who might benefit. What you may not realize, though, is Google trackers are actually lurking behind the scenes on 75% of the top million websites. To give you a sense of how large that is, Facebook is the next closest with 25%. It’s a good bet that *any random site* you land on the Internet will have a Google tracker hiding on it. Between Google and Facebook, the two of them, they are truly dominating online advertising, by some measures literally making up 74% + of all its growth. A key component of how they have managed to do that is through all these hidden trackers.

Some of your information has been exposed because of inept security measures. Some of your information has been exposed because you willingly gave it away (explicit or implied).

Control those things you can, and keep the surprises to a minimum.