November 2015

Visit our website at www.pcs4me.com Ken Johnson, Newsletter Editor

CALENDAR

SIG = Special Interest Group

This Week's Schedule

November 14 - Saturday - 1:00-3:00 PM
General Meeting - Leader: Phil Ball
Location: Prescott Public Library

Phil Ball will present Tips and Tricks with insights into various topics that assist with regular computer activity.
In addition to the presentations, the following are typical events which take place at our General meetings:

1) We hold an informal Flea Market in which you are encouraged to bring in your excess computer equipment or software and make them available for others to enjoy at no charge. Please deposit give-away items on the table in the back marked "Free Stuff." Any items left here at the end of the meeting are subject to disposal.

2) If you have items that are just too good to give away, you may set up a separate table and hold your own sale.

3) We conduct a raffle of gift cards at the end of the meeting, so make sure to get a pair of tickets from whoever is in charge and place one on the item you'd like to win.

4) We will also accept your used ink and toner cartridges for recycling. They are turned in to Think4Inc for credits which PCS uses to purchase office supplies from them.

Future Meetings

November 21 - Saturday
There will be no PCS meeting today.

November 28 - Saturday
There will be no PCS meeting today.

December 5 - Saturday

There will be no PCS meeting today.

Calendar *Cont on Pg 2*

December 8 - Tuesday - 6:00-8:30 PM
Board of Directors meeting - Private facility

Please contact Ray Carlson for information.

December 12 - Saturday - 1:00-3:00 PM
General Meeting - Leader: Ray Carlson
Location: Prescott Public Library

Note that these dates are correct at time of publication but are subject to change.
Up to date information can be found on our website, www.pcs4me.com

Unless otherwise noted, our meetings are usually held in the
Founder's Suite at the Prescott Public Library.

Welcome to
NEW MEMBERS

Kyle Baudek, Mary Brotchner, Richard Cesario, Donna Fazzio and Chuck LeRoy

Prescott Computer Society
Officers & Board of Directors
2015-2016

Officers:		**General Directors:**	
President	Ray Carlson	Joan Baum	Murray Smolens
Vice Pres	Phil Ball	John Carter	Dick Mason
Secretary	JB Burke	Ken Johnson	
Treasurer	Edi Taylor-Richards		

How to Set Windows 10 Privacy & Security Options

Sandy Berger, CompuKISS

www.compukiss.com

sandy (at) compukiss.com

Windows 10 has many Security and Privacy options that you can quickly and easily change. In fact, you have more control over these options in Windows 10 than you do in most other operating systems. Want to get started? Just follow these simple instructions.

Once Windows 10 is up and running, you can still set many of the Security and Privacy options. Just click on Start and go to the Settings, then click on the Privacy control panel icon.

You will see a long list of options and you can turn each of these off if you like.

In the Privacy area you can even quickly turn off the camera, microphone, and location information. And you can stop sending some information to Microsoft. Click on “Manage my Microsoft advertising and other personalization info” and you will get more information on how that works and also get the ability to turn off targeted ads.

Actually Windows 10 gives you more control of the privacy options than most other operating systems. As far as privacy goes, Windows 10 is no better or worse than many of the other operating systems that you use on your other connected devices. Yet, if you use Windows 10, you should check out the Privacy and Security options. **Ω**

What are Websites Doing with Your Personal Information?

By Ira Wilsker, *Assoc. Professor, Lamar Institute of Technology; technology columnist for The Examiner newspaper www.theexaminer.com; deputy sheriff who specializes in cybercrime, and has lectured internationally in computer crime*

REFERENCE WEBSITES:
http://www.govtech.com/data/How-Do-Websites-Use-Your-Data.html
https://identity.utexas.edu/privacycheck-for-google-chrome
https://identity.utexas.edu/idwise
https://identity.utexas.edu/strategic-partners
https://chrome.google.com/webstore/detail/privacycheck/poobeppenopkcbjejfjenbiepifcbclg
https://www.ghostery.com

You have likely noticed that the banner ads and other forms of advertisements on many of the web pages visited appear to "coincidently" be for many of the same items that you have recently searched for online. You may even notice that many of these ads are also from many of the same online sellers whose web pages you have recently visited. In some cases, you may also see online ads for direct competitors of previously visited websites, offering many of the same or similar products that you have looked at on other websites. It should not be surprising that the owners of many websites, as well as many third party advertisers, use a variety of tracking technologies to gather information on you, as an individual, the types of websites that you visit, and the products and services viewed. While many users find this targeted advertising interesting and useful, and even possibly necessary in order to support "free" web sites and online services, many others consider the gathering of such personal information as a gross violation of personal privacy.

Some of the more common methods of compiling and distributing this personal information and shopping preferences are the placement of "tracking cookies" on the user's device; web bugs or web beacons (small graphic files which transmit information when opened, often 1 pixel in size); and the dissemination (sale) of personal information entered on a website. Cookies are small, alpha-numeric and text based pieces of data which are by default, placed on the hard drive or other storage of the device being used to view a website; while some types of cookies are benign and necessary to compile shopping carts, store passwords and other login information, and save other information that can speed the web process, some other types of cookies may not be so desirable.

The most common type of unwanted cookies is often known as "tracking cookies", which are typically placed on the hard drive or other storage medium, just as other cookies, but these cookies can also be read by other third parties as a method of gathering information about the user, mostly for targeted marketing purposes. There are many companies that have a lucrative and highly profitable business selling access to the tracking cookies which they have

Continued on pg 4

Continued from pg 3:

previously placed in storage, most often by simply visiting a web page. Almost all browsers give the users the option to control which cookies can be saved and accessed, but the default is to accept all cookies. Tracking cookies that are currently saved in the device storage can often be easily and quickly removed by most of the reputable (and often free) security scanners, such as Malwarebytes (malwarebytes.org) and SuperAntiSpyware (superantispyware.com).

What many users might find shocking is that they unknowingly and explicitly allowed many of the websites that they visit to place tracking cookies and other marketing information on their computers and smart devices. When I mention this to users at some of my security and privacy presentations, some of those present get very agitated, and vehemently deny that they ever gave permission for websites to place such information on their computers and other devices. My typical response is something to the effect of "Did you ever read the privacy statement on those websites when displayed, or simply click on the "I Agree" box when first visiting them?" Most of the honest, but still aggrieved users, acknowledge that they never fully read the privacy statements on the websites visited, with the typical response being that the privacy statement is too long to read, or it is written in "legalese" which they cannot readily understand, so they simply "agree" in order to get access to that particular website.

Complex privacy statements, often blindly agreed to, have been a popular tool to legitimize the placement of that website's or other third party commercial tracking information on your computer, smart phone, tablet, or other device. These tracking devices are often a significant source of revenue for the website owner, and are often utilized by some of the largest and most reputable online vendors. In a recent article by Omar L. Gallaga, of the Austin American-Statesman, dated May 11, 2015, and reprinted by "Government Technology", Gallaga wrote, "How Do Websites Use Your Data? A new tool in Google Chrome puts website privacy policy language in plain English, letting you easily know whether your email address is shared or the site has access to your Social Security number, and if it tracks your location."

This free new tool, currently only available for Google's Chrome browser, is "PrivacyCheck", a Chrome browser extension (plug-in) which was developed by the Center for Identity at the University of Texas - at Austin (identity.utexas.edu). According to the Center for Identity, "PrivacyCheck is a browser add-on intended to provide consumers an overview of the ways in which companies use their personal data in a graphical, 'at-a-glance' format. ... PrivacyCheck surpasses existing add-ons, apps, and certifications by using a Data Mining algorithm to access the text of any webpage.

The user provides the URL for the company's privacy policy and PrivacyCheck searches the page, returning icons that indicate the level of risk for several types of PII (Personally Identifiable Information)". PrivacyCheck can be downloaded for Chrome from the Chrome web store at chrome.google.com/webstore, and entering "PrivacyCheck" in the search box. The latest version of PrivacyCheck, as I am typing this, is version 1.0.5, dated May 14. It is important to know that federal and state laws require businesses with a web presence to post their privacy policies, and there are often harsh penalties for violating those posted privacy policies.

To use PrivacyCheck to determine the degree of privacy risk on a particular web site, download and install PrivacyCheck from the Chrome web store (chrome.google.com/webstore). Once installed, open the selected website using the Chrome browser, and locate the privacy statement, often linked at the very bottom of the webpage; open the privacy statement page. On the top right of the Chrome address bar is a small icon which is light brown in color, and has what appears to be a lower case "i" within a brown circle; click on that icon. Once clicked, "Browse to a privacy policy and click Start". Within seconds a series of 10 larger icons will appear, with an easy to comprehend green, yellow, and red coloration, indicating the degree of privacy risks associated with that privacy policy and website.

Moving the cursor over each of the large icons will explain what it represents: the "envelope" icon represents what the website does with the user's email address, red indicating that the website uses, sells and shares the email address to others; the second icon represents the magnetic stripe on a credit card, and indicates what the site does with credit card information; the three asterisks "***" represent what is done with the user's social security number, green indicating that it is not collected or otherwise used; the "megaphone" indicates the marketing use of your private information, red indicating that the website sells your information to others for marketing purposes; the "compass" icon indicates what the website does with detected location information, red indicating that the website sells the user's location information to third parties; the sixth icon, circular with

Continued on pg 5

Cont'd from page 4

two eyes, indicates the policy on information gathered from children; the "badge with star" icon indicates the distribution of information to law enforcement, red indicating that the site will provide information to law enforcement without a warrant or subpoena; the "open book" indicates the policy on posting privacy policy changes and giving the opportunity for users to opt-out; the "pie chart" icon indicates whether or not the user can modify his own information; the tenth icon, which looks like a cloud with directional arrows, indicates what the website does with aggregated information, yellow indicating that aggregated information is distributed, but personally identifiable information has been removed.

PrivacyCheck is an excellent method to determine what commercial websites are really doing with your personally identifiable information (PII), but its major weakness is that it (currently) only works with the Chrome web browser. Users of other browsers may find some privacy utilities that provide significant privacy protection while online.

On all of my PCs, as a browser add-on, I have been using a free, popular browser extension called "Ghostery" (www.ghostery.com), which will seamlessly run on computers using any of the major and popular browsers including Firefox, Chrome, Opera, Safari, and Internet Explorer, as well as on mobile devices running the Android and iOS operating systems. According to its website, Ghostery claims to have, "The largest tracker database on the internet, constantly growing; Ghostery has the largest tracker database available on the web. We meticulously select, profile and cull over 2,000 trackers and 2,300 tracking patterns." Ghostery displays the tracking information on almost every web page opened, and gives the user the ability to allow or block trackers as desired.

Our personal privacy should be taken very seriously. Once third parties have access to our personal information, it is virtually impossible to get it back. Most of the browsers offer an option or setting to control privacy, which may be called "Do Not Track", "Reject Third Party Cookies", or some similar name. By using PrivacyTracker, Ghostery, browser privacy settings, and other utilities, our individual

Need Help With Computers?

Did you know that the Prescott Public Library has a program of Computer mentoring on a one-on-one basis? They have several experienced volunteers who will work with you using one of the Library computers.

All you need to do is make an appointment with either the "Ask a Librarian" personnel or go to: http://www.prescottlibrary.info/.

Is Windows 10 Spying on Us?

Sandy Berger, CompuKISS

www.compukiss.com

sandy (at) compukiss.com

Is Windows 10 spying on me? I have been asked this question over and over. My answer may surprise you!

There has been considerable publicity about Windows 10 being used as a spying tool for Microsoft. Blogs and even some fairly reputable websites have jumped on this bandwagon. Most of this publicity is aimed at making headlines to increase readership. As you well know, today's news is dominated by racy headlines, even if they are sometimes trumped up. Some of this bad Microsoft publicity is focused on increasing public paranoia to sell products.

One of my followers recently sent me a copy of an audio interview of Dr. Katherine Albrecht in which she trashed Windows 10 in an article entitled "Windows 10 is full blown electronic tyranny." Dr. Albrecht is a very intelligent, articulate, and well-educated lady. In this interview she says that Windows 10 keeps the microphone turned on all the time to bug homes and offices across the country. She says that Microsoft is making a copy of every file you create with Windows 10. However she also uses this interview to promote her Startmail product which is supposed to keep you safer.

Let's see if I can negate a few of her claims. First, Windows 10 uses your microphone to let you verbally communicate with Cortana, their new virtual assistant. Cortana is not listening all the time unless you change the settings and request that she does so. With the default settings, Cortana will only listen when you press the microphone button just like you would press the home button on an iPhone or iPad to ask Siri a question. Also, it is very easy to turn Cortana off or alternately to turn off your microphone completely.

Dr. Albrecht also says that Microsoft is sending the entire contents of all Windows 10 hard drives to their servers. Simply put, Microsoft is not copying all your files or documents. In the last month Windows 10 has been installed on 75 million devices. If Microsoft were to keep a copy of every one of those hard drives, we would be talking about thousands of Petabytes of data.

Continued on pg 6

Continued from pg 5

To give you an idea of how much data that is, it is estimated that the entire written works of mankind from the beginning of recorded history in all languages would take up about 50 Petabytes. Simply copying that amount of data would take years plus an astronomical amount of storage space and electricity.

Another complaint is that Windows 10 can be set up to share Wi-Fi passwords. Again this is not turned on by default. You must choose to use it, and when you do, you must authorize it and the passwords are encrypted.

I can sum up the reality of this situation in one simple statement. With Windows 10, Microsoft is doing no more snooping, spying, or collecting data than other large companies like Apple, Google, and Amazon. I have read the Microsoft Services Agreement, the Windows license agreement, and the Microsoft Privacy Statement carefully. I have also looked at several privacy documents from Google and Apple. They all have similar clauses.

The bottom line is that if you use any cloud storage like Microsoft's One Drive or Apple's iCloud, if you use an online email system like Gmail, Outlook, etc., or if you use services to sync your documents between computers and/or mobile devices, there is a copy of your data out there in the Cloud. Your cell phone provider, your ISP, your cable provider, your smart TV, and even your car knows a lot about you, as well. Facebook, Twitter, Instagram and other social media sites probably know more about you than you might ever expect. Most companies are using your data to learn more about you, whether to give you better service or to send you targeted ads. If they are subpoenaed, they will give your information to the lawful agencies, but then if you have drawn that kind of attention to yourself, those agents may be busting down your door and seizing your computers as well.

Right now Microsoft, Google, Apple, and Amazon are not spying on you or willfully giving the contents of your hard drive to anyone. Of course, an entire company could go bad, but currently you are at more of a risk from the bad guys and hackers than you are from the major companies. There are a lot of really good security people constantly monitoring the dealings of all the major companies.

So don't worry about Windows 10. It is no worse than Windows 7 or Mac OS X. If you want to be more secure, don't subscribe to any cloud services, don't use online email, and don't expect your data to sync between devices. If you want to be really secure don't access the Internet on your computer or tablet, don't use a cell phone, and don't buy a smart TV or any of the new Internet-connected devices, including a car.

Of course, if you do that you will be going back in time about 30 years. I know I wouldn't want to give up the knowledge, connectivity, productivity or entertainment that we have gotten from these devices. **Ω**

Prescott Computer Society
Where you share what you know,
and learn what you don't.