

Bits of Bytes

Newsletter of the Pikes Peak Computer Application Society, Colorado Springs, CO

Volume XXXV

June 2015

Issue 6



Meeting Minutes

by Toni Logan,
Secretary,
P*PCompAS

President Cary Quinn called the 2 May 2015 meeting to order at 9 a.m. He announced that the coffee is free to one-time guests and a donation from all others. The coffee is compliments of Laura at Starbucks at Citadel Crossing.

The minutes were approved as printed in the newsletter.

OFFICER REPORTS

The Vice-President was not in attendance, but the program for today is on Windows 10 and next month will be a presentation by the Sheriff's Department on Security.

Treasurer Dennis Conroy reported that we have \$6741.30 in the treasury, which this month included a small dividend from the credit union.

Membership Chairwoman Ann Titus announced that we have a new member, Tim Hoffman, who is in ISSA. Stanley Rapaport introduced his daughter, Kathleen Bucher, who is visiting. Also our new member Tim Hoffman introduced his guest, Cal Swartz.



New member Tim Hoffman is mugged by Ann Titus

Next P*PCompAS meeting: Saturday, 6 June 2015

We may have the Sheriff's Department on hand to talk about computer forensics and security. Watch our Website for last minute details.

Editor Greg Lenihan reported that the deadline for the next newsletter is Saturday, May 23. He also distributed several printed editions of the newsletter.

APCUG Representative Joe Nuvolini reported that there will be a conference in September in Las Vegas. There is a cruise in January to the western Caribbean, Miami, the Bahamas and Grand Caymans. Joe will write a short item about the club for the next Q2 Report for Region 9, of which we are a part.

OLD BUSINESS

We need volunteers to present programs during our meeting. If you have anything you would like to present, contact VP Harvey McMinn or President Cary Quinn.

NEW BUSINESS

The President announced that he was working on organizing some mini-programs where members would show off a favorite app. The date of the July meeting which lands on the 4th was discussed and it was suggested to ask if the church was available on July 11. The church gift is on hold until we find an appropriate one. See Ilene Steinkruger if you want to do a book review. It was also suggested that we advertise in the local media and also with other groups.

AROUND THE ROOM

See the Website for the audio

of this portion of the meeting, or visit <https://app.box.com/s/bg5mii07qnu86x7zuw56dr9tt5752wyu>.

PROGRAM

John Pearce presented an outline of the new Windows 10 operating system. Windows 10 will be a free upgrade within a year of its release for those with Win 7 or Win 8.1.



John Pearce presenting in May.

DRAWING

Paper—Pat Krieger
Earbuds—Bob Blackledge
Deck of Cards—Cary Quinn
Microphones—Dennis Conroy ☺

In This Issue

Articles

3 Things That Spy on You.....	8
How to Stream Video.....	7
Nuggets from Nuvo.....	3
Nybbles and Bits.....	2
Recording Sound From Your PC	6
Websites & Your Personal Info	4

P*PCompAS

Meeting Minutes	1
-----------------------	---



Officers

President: Cary Quinn
cary.quinn@gmail.com

Vice President: Harvey McMinn
harveys_homes@yahoo.com

Secretary: Toni Logan
bradtonlogan@gmail.com

Treasurer: Dennis Conroy
dennisconroy@comcast.net

Staff

APCUG Rep/Webmaster: Joe Nuvolini
Editor: Greg Lenihan
Librarian: Paul Major
Membership: Ann Titus

Committees

Hospitality: Pat Krieger
Programs: Paul Godfrey, Toni Logan, and Peter Rallis
Publicity: Harvey McMinn
Nominating: Vacant

Board of Directors

Toni Logan
Norm Miller
Bob Blackledge
Warren Hill
John Pearce

Nybbles and Bits

by John Pearce, P*PCompAS

The number of unwanted phone calls, probably solicitations, at my house seems to be growing out of control. My wife and I have taken the approach that if we don't recognize the caller ID, we don't answer the phone. We expect if it is someone we know and we don't answer, they will leave a message. There are two small problems with this approach: there have been a few calls that we should have answered and didn't, and second, the phone continues to ring until the answering machine picks up the call. That started a search for a better solution.

One service I found is Nomorobo (www.nomorobo.com). It looks like a great service however it is generally limited to VoIP (voice over IP) phone service. The service relies on a feature called simultaneous ring, where both your phone and the Nomorobo service receive the ring signal and the caller ID information at the same time. Nomorobo does its thing and if it is a known spam/solicitation call, will quickly answer the phone and hang up.

We have a traditional wire line phone from CenturyLink and don't have an interest right now in porting to a VoIP provider. I thought about just disconnecting the analog phone line and relying on our cell phones. When I started making a list of all the places to contact for changing the phone number, the work involved is more than I want to do, at least right now. We have had the same home phone number for almost 25 years.



That left me with searching for a way to block incoming phone calls. CenturyLink has several extra cost options. Anonymous Call Rejection stops ANONYMOUS and PRIVATE calls. According to CenturyLink, OUT OF AREA, UNAVAILABLE, UNKNOWN or NOT PROVIDED calls cannot be blocked. They also have Call Rejection which blocks specific phone numbers. There is a limit of 10 phone numbers with Call Rejection or 25 numbers with Enhanced Call Rejection.

An Internet search for call blocker turned up a number of products. These devices plug into your home phone line and require caller ID service from the phone company. They claim to have the ability to block calls if a phone number is not provided, or block calls for a complete area code or the combination of area code and exchange (first six digits of a complete phone number). One product claimed it could block up to 1,200 individual phone numbers. One benefit is that the call blocker can be connected between the wall jack and the phone and you will not hear the phone ring if the call is blocked.

One particular advertisement mentioned call blocking with certain brands of answering machines and included Panasonic. A little more

Continued on page 3

The Pikes Peak Computer Application Society newsletter is a monthly electronic publication. Any material contained within may be reproduced by a nonprofit user group, provided proper credit is given to the authors and this publication, and notification of publication is sent to the editor. Any opinions contained in this newsletter are made solely by the individual authors and do not necessarily reflect or represent the opinions of P*PCompAS, its officers, or the membership. P*PCompAS disclaims any liability for damages resulting from articles, opinions, statements, representations or warranties expressed or implied in this publication.

P*PCompAS welcomes any comments, letters, or articles from members and non-members alike. Please send any articles to the editor (see last page for address). The editor reserves the right to reject, postpone, or edit for space, style, grammar, and clarity of any material submitted.

The time finally came to replace my old XP desktop computer. It has served me well for over ten years. I decided to change to a Windows 7 Dell computer I bought some time ago for that purpose. I installed the apps I use most frequently on the new computer, as well as moving my data files over. I also copied my latest Acronis True Image backup files of my old XP machine over to a spacious E drive where I backup the Dell. They are invaluable. Here's why: If I find I am missing a file that was on the old XP computer, I merely double-click on the old backup file (tib) and it launches in Windows Explorer. So I need only locate the file I want and copy it over to the Dell. I have had to do this on a number of occasions. What a great feature.

I also decided to pick up a new UPS for the Dell. I bought a CyberPower unit from Best Buy. Rather than toss the old UPS, I took the old battery down to American Battery on Platte Ave and picked up a new one for a bit over \$20. I put the old UPS on the computer I use as a server. Buying a new battery is a



Nuggets from Nuvo by Joe Nuvolini, P*PCompAS

lot cheaper than buying a new second UPS. When I worked at the Income Tax Center we always bought replacement batteries from American. I also found that there is a new software package available for CyberPower UPSs. It is called CyberPower Power Panel Personal Edition. It works with the old units that connect via USB cable to your computer. You can download it by visiting www.cpsww.com and navigate to the software section.

I found that my old Adobe Acrobat PDF ver 4 printer driver won't work on Windows 7. I hunted around and found doPDF on Kim Komando's download area. If you are looking for a PDF printer driver go to: <http://www.komando.com/downloads/742/an-easy-way-to-create-pdfs>.

APCUG has launched their new Website at www.apcug2.org. As best I can see, it requires no login. You can access APCUG Reports, current and old issues, Push articles, the Speakers Bureau and a wealth of other info. It also has info on upcoming APCUG events. It's worth a look-see. ☺

Nybbles (Continued from page 2)

searching and I found there is call blocking capability in the Panasonic cordless phone with the answering machine that I currently use. It will block up to 30 numbers and there is also an option to block incoming calls without a phone number.

By the way, I do not recommend turning on blocking for calls without a phone number. From personal experience, I found the emergency room phones at both Penrose and Memorial hospitals block the phone number. It has been several years since I received one of those phone calls so it is

possible things have changed.

Incoming calls ring just once if the caller ID number is listed in call blocking. The answering machine answers the phone then hangs up. The caller ID list has a symbol beside the number to indicate it is in the call block list. So far, this has worked fairly well. ☺



The digerati congregated at the Country Buffet on May 16th to keep up with tech and generally keep dry between scattered showers, in what was a very wet May.



What are Websites Doing With Your Personal Information?

Published with permission from Ira Wilsker, Golden Triangle PC Club, columnist for The Examiner, Beaumont, TX

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/poobeppenopkcbjefjjenbiepifcbclg>

<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 “coincidentally” 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 have previously been 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.

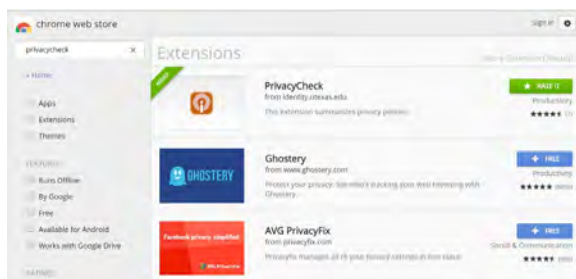
Complex privacy statements, often blindly agreed to, have been a popular tool to legitimize the placement of that website’s or other third party commercial tracking information on your computer, smart phone, tablet, or other device. These tracking devices are often a significant source of revenue for the website owner, and are

Continued on page 5

Personal Information (Continued from page 4)

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 e-mail 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 e-mail address, red indicating that the website uses, sells and shares the e-mail 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 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

Continued on page 6

How to Record the Sound Coming From Your PC (Even Without Stereo Mix)

By Chris Hoffman, reprinted with permission from HowToGeek.com

Original article at: <http://www.howtogeek.com/217348/how-to-record-the-sound-coming-from-your-pc-even-without-stereo-mix/>

You don't have to hold up a microphone to your computer's speakers to record its audio. Even if you don't have a Stereo Mix option on your PC, you can easily record the sound coming from any Windows PC.

This can all be done with software. No, you don't even need to connect your computer's audio output to its audio input with an audio cable to do this — although that is an option.

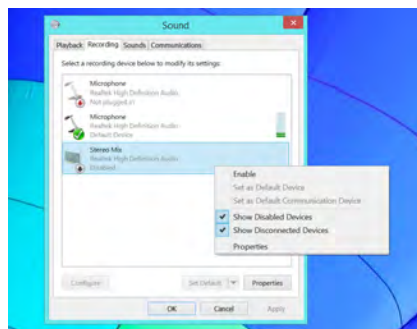
Option 1: Stereo Mix

Stereo Mix is sometimes called "What U Hear." It's a special recording option that may be provided by your sound drivers. If it is, you can select it (instead of a microphone or audio line-in input) and force any application to record the same sound that your computer is outputting from its speakers or headphones.

On modern versions of Windows, Stereo Mix is generally disabled by default — even if your

sound drivers support it. Follow our [instructions to enable the Stereo Mix audio source on Windows](#). Use any audio-recording program and select "Stereo Mix" as the input device instead of the usual "line-in" or "microphone" option.

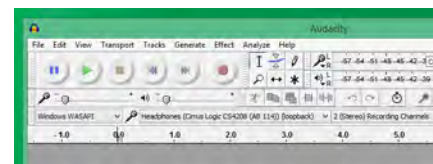
On some devices, you may not have this option at all. There may be a way to enable it with different audio drivers, but not every piece of sound hardware supports Stereo Mix. It's become less and less common.



Option 2: Audacity's WASAPI Loopback

Don't have a Stereo Mix option? No problem. [Audacity](#) has a useful feature that can record the audio coming out of your computer even without Stereo Mix. In fact, Audacity's feature may be even better than Stereo Mix — assuming you're willing to use Audacity to record the audio, of course. This takes advantage of something Microsoft added in Windows Vista, and it'll also function in Windows 7, 8, 8.1, and 10. It helps make up for the lack of a Stereo Mix option on modern Windows PCs.

In Audacity, choose the "Windows WASAPI" audio host and then an appropriate loopback device — for example, "Speakers (loopback)" or "Headphones (loopback)."

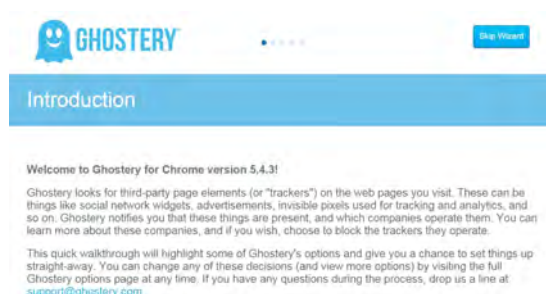


Continued on page 7

Personal Information (Cont. from page 5)

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 privacy may be better protected. ☺

How to Stream TV

By Sandy Berger, CompuKiss, www.compuKiss.com

There is no doubt that the world of television content and the way we get that content is changing. Many people are “cutting the cord” by turning their backs on cable and satellite TV. These folks are turning to streaming TV shows and movies. For those of you who are not yet familiar with “streaming,” here’s a quick tutorial on how to stream and what you need.

Streaming is named for a technique for transmitting data over the Internet so that it can be processed as a steady and continuous stream. This differs from downloading content in which the entire chunk of data must be downloaded before it can be processed. Most users do not have enough bandwidth to download an entire movie or TV show, so streaming is a great technique. During streaming the content is constantly being processed so you can watch the show while it is being processed with no interruption.

Streaming allows you to watch television shows and movies without having a cable or satellite subscription. You can use streaming to

augment a basic cable or satellite TV subscription or to eliminate cable or satellite subscriptions completely making it a valuable tool for TV watching.

Also, Netflix and Amazon are now producing their own programming, much of which, like House of Cards, has become very popular. With streaming you can also watch a wide variety of movies and the past episodes of many different TV shows.

Even if you are not technically inclined, you will find that streaming is quite simple to setup. Here’s what you need.

First -- an HDTV with an HDMI port. While older analog TVs can also be set up to stream, having an HDMI port make it much easier. All HDTVs, which include most newer TVs, have these ports. To find them, look at the back of the TV; they are usually labeled HDMI.

Second -- You need a good broadband Internet connection. This is how the data (movies) will get to your television. The faster the better and you might want to upgrade your Internet, but you may not have to. Try it with the connection you have right now. You

Continued on page 8

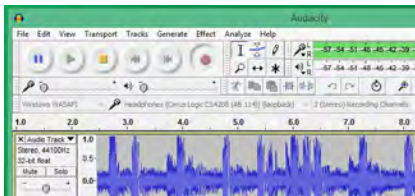
Record Sound (Cont. from page 6)

Click the Record button to start recording the audio in Audacity, and click Stop when you’re done. Because you’re using Audacity, you can [easily trim and edit the sound file](#) when you’re done.

Audacity’s tutorial website explains why this feature is actually better than Stereo Mix:

“WASAPI loopback has an advantage over stereo mix or similar inputs provided by the soundcard that the capture is entirely digital (rather than converting to analog for playback, then back to digital when Audacity receives it). System sounds playing through the device selected for WASAPI loopback are still captured, however.”

In other words, your recorded sound file will have be higher-quality when using Audacity’s WASAPI loopback option.



Option 3: An Audio Cable

There’s always the low-tech solution, although it’s a bit of a dirty hack. Just get [an audio cable with a male 3.5mm connector on both ends](#). Plug one end into the line-out (or headphone) jack on your PC and the other one into the line-in (or microphone) jack on your PC. You’ll stop hearing the sound your computer produces, but you can use any audio-recording program to record the “line in” or “microphone” input. To actually hear the sound, you could get a [splitter](#) and output the audio to headphones or speakers at the same time you direct it back into your computer. Sure, this is inconvenient and silly

compared to to the above options. But, if you desperately need to capture the audio coming out of your computer in an application that isn’t Audacity and you don’t have Stereo Mix, the cable will allow you to do this.



Obviously, copyright laws may prevent you from distributing whatever recordings you make in this way. Don’t use these tricks for piracy! After all, even if you were going to pirate some audio, there’d be much easier ways to do it than this. ☺

3 Surprising Things That Spy on You That You Can't Stop

by Kim Komando (tip from 8/9/14)

Copyright 2014. WestStar TalkRadio Network, reprinted with permission. No further republication or redistribution is permitted without the written permission of WestStar TalkRadio Network. Visit Kim Komando and sign up for her free e-mail newsletters at: www.komando.com

Do you ever feel like you're being watched? In the past, you could chalk it up to paranoia, close the curtains, and get on with your life.

Thanks to technology, it's not just your imagination. You really are being watched in your home, at work, and everywhere in between.

From online advertisers and

hackers to the NSA and other government agencies, everyone is trying to keep tabs on you. And things keep getting worse.

If you think you know every gadget and organization that's a danger, think again. Here are three things spying on you that you probably didn't know and that you can't stop.

1. Your car

You may or may not have heard that beginning September 1, 2014, every new car is required to have a black box installed. This will record information about your speed, direction, braking, whether you're wearing a seat belt and everything else going on in the

Continued on page 9

Stream TV (Cont. from page 7)

might be pleasantly surprised.

Third -- you need a streaming media device. Some newer TVs and most Blu-ray players can access the Internet. If you have one of these you can use it as your media streaming device.

If you don't have one of these, you will need to purchase a new device. The good news is that these devices are small and inexpensive. These devices include Chromecast, Roku, and Amazon Fire TV and Fire Stick. They range in price from \$30 to \$100. I have tried them all and they all work quite well. If you already belong to Amazon Prime, an Amazon Fire might be the best choice. To get the best selection of content, Roku is the best. In any case, the main difference in price is often whether the device comes with a remote control or not. If it doesn't come with a remote, like the Chromecast, you will have to use a tablet or mobile phone to control it. If that doesn't appeal to you, opt for one with a remote.

Fourth -- you will need a wireless router. Although some devices can hook up directly to your wired Internet router, in most cases your television is not in the same room as the Internet connection making it necessary to have a wireless router to transmit the data wirelessly to your television. If you already have wireless in your home for a tablet or phone, you are all set.

When you get your streaming media device home, you simply plug it into the TV. Set the TV to the proper input like HDMI 1 or HDMI 2, then follow the set up instructions that will appear on the screen. All are easy to follow. The only thing you will need is to know the password for your

wireless network if it is password protected.

After the setup, you will see your choices of things to watch. Some of these will be free, some will have extra costs. For instance, Netflix and Hulu both have a ton of content, but each charges about \$10 a month. Fortunately both have free trials which you can use.

Watching streaming media on your TV is not as simple as watching cable TV. There are little inconveniences. Every time you want to switch to your streaming device, you have to change the input on your television. Also there is no simple guide as the one you get with cable or satellite TV. You often have to search for what you want to watch. The Amazon Fire TV (not the Fire Stick) makes this easier because its remote has a voice search which works quite well. Just speak the name of a movie, actor, or director and it will find the movie you want. This, however, only works for Amazon Prime movies and shows. Also, if you have more than one subscription, you have to remember which movies are on which service....Now was *Orange is the New Black* on Netflix, Hulu, or Amazon?

Yet, the inconveniences are minor and there are advantages. For instance, after I started streaming, I was able to watch the entire series of *Downton Abbey* on Amazon and *House of Cards* on Netflix at my convenience. How wonderful to watch a few episodes a week until I got caught up!

If you haven't yet tried streaming, be sure to check it out. You may find a new way of watching television that can save you money and give you new options. ☺

Things Spying on You (Cont. from page 8)

seconds surrounding a crash.

Investigators will know exactly what happened rather than trying to figure it out based on witness testimony. That might not be such a bad thing—if you're in the right.

Of course, the big worry is that the black box might eventually go beyond that. Paired with a GPS, a black box could easily record your entire driving history.

Insurance companies might eventually use the data to set your premiums. Some states, such as California, are already talking about including GPS to tax drivers based on how many miles they drive. What happens if hackers get hold of the data?

"Well," you might say, "I'm not going to buy a car made after 2013." I have some bad news for you. Around 96 percent of new cars already include a black box. In fact, they've been in use by some manufacturers since the early '90s. If your car has one, it will say somewhere in the owner's manual.

Of course, it might not matter when self-driving cars finally take over the road.

2. Your favorite stores

Whenever you swipe a loyalty card, enter your phone number, or use the same card at a store, your purchases go into a database profile. Based on what you buy, stores know way more about you than you think.

Back in 2012, the New York Times Magazine reported a shocking story. A father went ballistic in a Target after the store sent his 16-year-old daughter coupons for baby supplies. What was Target doing sending pregnancy promotions to a minor?

Well, it turns out the daughter really was pregnant. Target had a team that, crunching data from millions of consumers, were eerily accurate at such predictions. Target can tell how far along a pregnancy is and estimate a fairly accurate due date based on what a person buys.

Imagine what else they can figure out about your politics, beliefs, health, relationships and more. Scary stuff.

Target isn't the only store doing this, of course. Any business loves to have an inside edge on its customers so it can time promotions for the most impact.

Of course, imagine if the government got hold of that information (assuming it hasn't already) or your health-insurance provider.

Even worse, what about identity thieves and scammers? Think what they could do with invaluable information into your habits.

Given the major data breaches happening lately, with Target coincidentally having the worst data breach in retail history, it isn't a stretch to think this information might get out as well.

And, aside from using fake information—which some people do — or shopping at the farmer's market, there isn't anything you can do about it.

3. Your Internet service provider

Quick: What's the one organization that knows everywhere you go online? If you read the title of the section, then you know the answer is your Internet service provider.

Not that it's necessarily trying to spy on you, but its business is connecting your computer to websites. And for various business reasons, it saves that information.

Some ISPs keep your traffic information for a few months and others for a year or more. And, of course, any ISP will turn the information over to law enforcement if asked.

There is a way around this. You can use a service like [Tor](#) or [KProxy](#). These route your traffic through servers around the world. No one can track where you're going.

I should point out that no routing system is foolproof and the government has cracked Tor in the past. So, do me a favor and don't use these proxy services for anything illegal. ☹

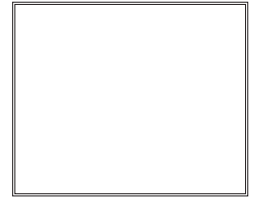
In Memoriam



George Gene Rothwell
May 10, 1936 - May 16, 2015

We were saddened by the loss of a long-time member last month, and our society wishes to express condolences and deepest sympathy to the Rothwell family.

P*PCompAS Newsletter
Greg Lenihan, Editor
4905 Ramblewood Drive
Colorado Springs, CO 80920
e-mail: glenihan@comcast.net



Coming Events:

Next Membership Meeting: 6 June, beginning at 9 am (see directions below)

Next Breakfast Meeting: 20 June @ 8 am, Country Buffet, 801 N. Academy Blvd.

Newsletter Deadline: 20 June.

Check out our Web page at: <http://ppcompas.apcug.org>

