Founded 1982
www.rcsi.org

The Rochester Computer Society, Inc.
a computer/tech club open to everyone

MONITOR

Vol. 36, No. 08 August 2018

"Your Computer User Group of the Air", Saturdays from 12:00 pm to 2:00 pm with Nick Francesco, Dave Enright, and Steve Rae. Broadcasting on JAZZ 90.1 FM from Rochester, NY.
Call 966-JAZZ (585-966-5299) or 800-790-0415

The RCSI '**Monitor**' newsletter can be found in most public libraries in Monroe County. *Free* copies can also be found in the following computer stores: Microworx, Just Solutions, TSC Electronics, and Pod Computers. Digital copies may be obtained from **www.rcsi.org** or my cloud storage at **http://tinyurl.com/tonydel-rcsi-newsletters/**.

Some Past Presentations:
Open Source and Free Software
Protecting Your Identity
Keeping Mobile Devices Secure
3D Printing, ENABLE project
Flash Drives-Not Just for Storage
Features, Mac OS X & Windows
Tablets, the Programs and Uses
Personal Finance Software
Amazing Browser Tips
Linux is Like Cars
Close up Photography

Member of apcug
An International Association of Technology & Computer User Groups

Tues, August 14
Our Annual Club Picnic, Henrietta Town Park

Tues, September 11
TBD

Tues, October 9
'Cyber Awareness Month' presentation
by Norbert (Bob) Gosticha, via Zoom

In This Issue

Facebook Files Patent For Exactly the Kind of Spying It Claims It Doesn't Do	Joel Hruska
How Nantes Team's 3-D Printing May Alter Shape of Homes to Come	Nancy Owano
Linux and Open-source Jobs are in More Demand Than Ever	Steven J. Vaughan-Nichols
Cryptomator: Encryption for Your Cloud Storage	Ask Leo!
Wi-Fi - 2.4 or 5GHz	Carol Picard
One Dongle to Rule Them and In the Darkness, Bind Them	Chris Woods
Nothing Bad Ever Happens	Greg Skalka

TSC Computer and Electronics Repair
Custom Computers - Electronic Surplus and Recycling
Home Service - Small and Mid Size Business IT Mgmt.
765 Elmgrove Rd, Ste 2
Rochester, NY 14624
Phone (585) 429-6880
Fax (585) 429-7671
www.tscelectronics.com

Special Interest Group

Linux Sig

The workshop is the **third Saturday of each month**, at Interlock Rochester, 1115 East Main St. www.interlockroc.org

Enter through door #7 on the end of building, near *Comics Etc* and Goodman St. Find 'Interlock' on the intercom directory to get buzzed in and go upstairs to suite #200. We have experts on hand to fix problems and answer questions about Linux and FOSS (free and open source software). Bring your system in so we can help you get the most out of it. Hope to see you there.

Free, **Virtual Technology Conferences**, ONLINE
presented by APCUG

Saturdays: 8/18, 11/3

For Conference Description & Registration Links, go to apcug2.org/category/ **virtual-tech-conference**

Facebook Files Patent For Exactly the Kind of Spying It Claims It Doesn't Do

By Joel Hruska on June 29, 2018

For years, Facebook users and journalists have noticed that the service has an unsettling habit of serving up advertisements related to topics they'd often been discussing in their personal lives or had no previous habit of Googling. The question of whether Facebook listens to conversations going on around us has come up so regularly, there's been a host of investigatory articles and discussions on the topic in 2018 alone. Facebook's position throughout all this has been consistent: The company claims it does not spy on users by using their smartphone mic to listen in on conversations. It has maintained this position officially since 2016.

But now we know one more additional piece of the puzzle. Facebook might not spy on you in this fashion today — but it wants the patent on spying on you in this way tomorrow.

In a patent application filed on June 14 and first discovered by the UK publication Metro, Facebook requested a patent on exactly the kind of system it has sworn that it never uses. The abstract reads:

> An online system analyzes broadcast content viewed by individuals in a household. Each individual in the household is associated with a client device on which a software application module is executed. When the software application module detects one or more broadcasting signals of a content item broadcasted to the household, the software application module records the ambient audio, including audio from the broadcasting device. The software application module sends an identifier of the individual associated with the client device, an ambient audio fingerprint derived from the recorded ambient audio, and time information for the recorded ambient audio to the online system. The online system, based on the ambient audio data, identifies the corresponding individual and content item and logs an impression for the content item upon determination that there was an impression of the identified content item by the identified individual.

RCSI Officers

Pres: Steve Staub 429-9877
srstaub1@rochester.rr.com
VP: Mark S. Lawson . . . 544-5377
mslawson51@peoplepc.com
Treas: Dennis P. McMahon
. 235-1260
denmac733@gmail.com
Secretary: www.rcsi.org
Help's Half Hour . . Jan Rothfuss

Board Members at Large

Tony Dellelo 734-6149
tonydel@techie.com, 9/21
Bob Avery 385-4491
webmaster@rcsi.org, 9/20
Jan Rothfuss 347-6020
jan_rothfuss@hotmail.com, 9/19

Standing Committees

Linux SIG: . . . Carl Schmidtmann
unixgeek@faultline.com
Programs and *Monitor* editor: . . . .
. . . . . Tony Dellelo
Webmaster: . . . . . Bob Avery
Membership: . . . . . Steve Staub

Planning Meeting

Held on 1st Tuesday of each month at 7 pm, at St. John's Meadows, Briarwood building.

Newsletter Printing

The newsletter was printed at St John's/Chestnut Court by the printing group, with the help of Don Wilder (computer and printer operator). *We will try and print on the 1st or 2nd* ***Thursday morning,*** *following the monthly meeting.*

The background of the patent application goes into yet more detail on this

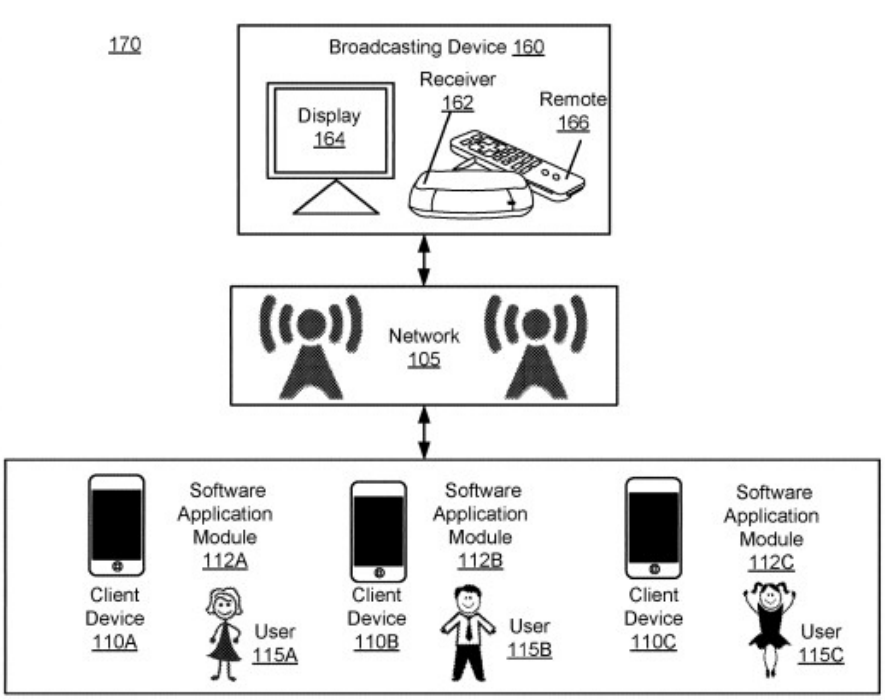


FIG.1B

roposed system, spelling out how, for advertising purposes, it would be advantageous for advertisers to know exactly how and when people are being exposed to their advertisements. It references the use of high-frequency audio being used to trigger this data collection (by embedding the audio within another video or audio stream), but doesn't necessarily depend on this activation method. Simply bringing a client device within range of a broadcasting device could also trigger the audio collection based on what the patent describes.

Either way, once you approach the broadcasting device, it would transmit a signal to the client device to begin collecting ambient audio data. Then it would search this data to determine what you were exposed to for the purposes of recording audience impressions.

Facebook's Response? We Won't USE the Patent

Facebook's frankly hilarious response to this latest discovery is to argue that sure, it filed for the patent, but it wouldn't, you know, *use* it. In a statement to Engadget, Facebook VP and Deputy General Counsel Allen Lo claims the patent was filed "to prevent aggression from other companies" and that "patents tend to focus on future-looking technology that is often speculative in nature and could be commercialized by other companies."

Facebook has long since exhausted any tenuous credibility it might once have deserved on any topic related to user privacy. Ever noticed that every time Facebook screws up — every *single* time — it's in the direction of providing less privacy, fewer protections, and weaker protections for your personal data than the company previously promised? From May 18 to May 27, 14 million Facebook users had their private posts mistakenly made public. Whoops. Facebook regrets the error.

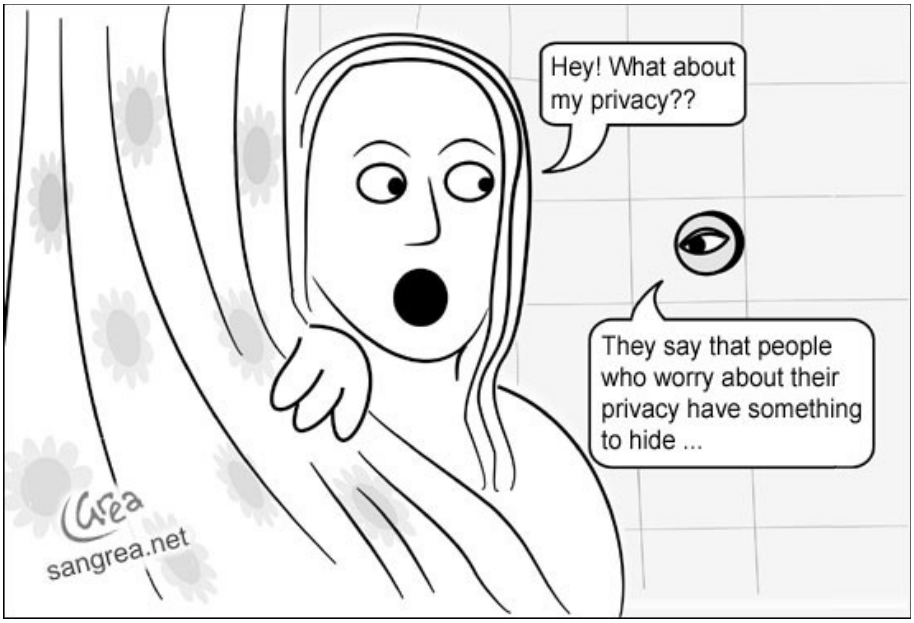
Facebook tracks the things you say. It tracks the things you don't say. It tracks you when you aren't on Facebook. It ships VPN applications that double as spyware. It's signed secret data-sharing sweetheart deals with various hardware manufacturers you never agreed to share your data with. It's profited from the wholesale abuse of its systems by companies like Cambridge Analytica. Mark Zuckerberg has been pulling from the same "sorry" playbook for literally the past 14 years in ways that make South Park's send-up of BP in the aftermath of the

Deepwater Horizon seem like a genuine apology. Mark Zuckerberg has never believed in privacy, not least because violating yours has made him one of the richest people on Earth.

Is it possible that Allen Lo is telling the truth? Absolutely. But at this point in the company's history you'd frankly be an idiot to believe him. At no point since its inception has Facebook given the slightest indication that it meaningfully cares about your privacy. In fact, the one and only thing you can bet on with regard to Facebook is that it's always about 15 minutes away from its next privacy-related scandal. Does anyone actually believe that a patent like this **won't** directly lead to "Facebook admits it gathered everything said inside homes for six weeks" types of headlines at some point in the future? Because if you do, you literally haven't been paying attention to the past decade of Facebook disasters. This is what happens when you combine "move fast and break things" with "actively corrode the very concept of privacy and declare it a social good." It's a feature, not a bug, at least from Facebook's perspective.

There are complicated reasons why you might recognize these facts and continue to use FB anyway. Maybe you value the benefits of being in touch with friends and loved ones more than you care about the privacy issues. Maybe you use FB professionally. Maybe you simply aren't all that concerned with privacy in the first place. But it's long past time to stop pretending that Facebook has or will ever treat user privacy with anything deserving of the phrase "respect." It never has. It never will. Pretending otherwise extends an objectively unearned benefit of the doubt to a corporation that's never deserved it.

Reported in Extreme Tech, June 29, 2018, www.extremetech.com.



Articles by RCSI members may be reprinted by other user groups, without special permission, provided they are unaltered and the publication emails a copy to the author. Articles by authors from other organizations retain their original copyright. Articles provided by the Association of Personal Computer User Groups (APCUG) may be reprinted if credits remain intact.

Computer Recycling

Some Residential Drop off Locations: **Call first**, to find out what is accepted, especially for 'tube type' tvs or monitors.

TSC Computer & Electronics Repair, accepts most electronic waste, including printers. Does not accept crt type monitors or tvs. They are located at 765 Elmgrove Road, Gates. 429-6880, www.tscelectronics.com

Microworx accepts most electronic waste (large monitors/crt's, 50 cents/pound), located at 20 Allens Creek Road. Brighton. 585-271-0050

Monroe County *ecopark* (Cathode Ray Tube TVs and monitors - $10 each, credit/debit card only) 10 Avion Drive
Rochester, NY 14624
Phone: (585) 753-7600 (Option #3)

How Nantes Team's 3-D Printing May Alter Shape of Homes to Come

by Nancy Owano, Tech Xplore, July 10, 2018

For some months now, a 3D printed house in Nantes has drawn lots of attention, not just because a printer was involved but also because it went up from start to finish so quickly (54 hours to print, then add some more time for the windows and roof). *Interesting Engineering* said it took some more time to add the roof, windows and doors. A robot printer was used to print layers from the floor upwards to form the walls, and videos show a beautiful result of five rooms with rounded walls.

Now comes the latest news of the world's first family to move into a 3D-printed home—that is now home for the Ramdani family, consisting of the two parents and their 3 children, to enjoy life in the 4-bedroom house in Nantes, France.

The innovator behind this is project leader Benoit Furet, a professor at Nantes University. In a BBC report, Furet discussed costs.

BBC's Michael Cowan went through the figures posed by Furet. "He thinks that in five years they will reduce the cost of the construction of such houses by 25% while adhering to building regulations, and by 40% in 10 to 15 years."

Reasons why 3D printed house prices will go down are that the technology will undergo refinements, and one can expect economies of scale as more houses are built.

The 1,022 square foot house was built to curve around the 100-year-old protected trees on the plot, Cowan wrote. That points to a key advantage in using 3D printing for construction—far richer solutions in shape, and a creative experience opens up for architects to think outside the "box" of straight walls and cookie-cutter boxed rooms that one sees in traditional constructs.

The present-day limits are especially glaring in traditional public housing. Residents' units look more like confined prison cells blocking out the natural outdoors, minus only the bars on windows.

The project leader said that 3D printing enabled richer solutions in terms of the shape of the house, with more interesting possibilities for architects then working with straight walls.

Curves are not only pleasing to the eye but also have practical advantages. "The curve also improves the home's air circulation, reducing potential humidity and improving thermal resistance," said Cowan.

Mashable carried an especially good video that delivers on one's visual impact of what this house achieves in design and function for a family of five. To view, go to https://mashable.com/2018/07/09/this-is-the-first-3d-printed-home-to-actually-host-a-family/#mR30Q77lmsqi.

The BBC walked readers through the building process(https://www.bbc.com/news/technology-44709534): A team of architects and scientists work on the idea and it is programmed into a 3D printer, which in turn is brought to the site of the home.

Work begins, printing in layers from the floor upwards. "Each wall consists of two layers of the insulator polyurethane, with a space in-between which is filled with cement." The walls are thick and insulated. Windows, doors, and roof are then fitted.

The house has an IoT system, as the video in *Mashable* showed, where the residents can control temperature and other features via tablet.

The 3D printed house has been a collaboration between the city council, a housing association and University of Nantes. From the town planning perspective, the officials are interested to see if the same housing principles might be able to be applied for other public buildings, such as sports halls. Can such efforts influence a shift in the building industry?

Time will tell. Reports said Fouret is working on a project in the north of Paris to print 18 houses and a commercial building.

Reported in Tech Explore (techexplore.com).

Linux and Open-source Jobs are in More Demand Than Ever

The Linux Foundation and Dice.com's 2018 Open Source Jobs Report shows the demand for open-source savvy employees is stronger than ever.

By Steven J. Vaughan-Nichols for Linux and Open Source

Do you want a tech job? Then, it's time to move away from Windows and head toward Linux and open source. According to The Linux Foundation and Dice's 2018 Open Source Jobs Report, 87 percent of hiring managers are having trouble finding open-source talent, while hiring open-source talent is now a priority for 83 percent of employers.

"Open source technology talent is in high demand, as Linux and other open source software dominates software development," said Linux Foundation's executive director, Jim Zemlin, in a statement. "I am encouraged that that companies are recognizing more and more each day that open-source technology is the way to advance their businesses. The Linux Foundation, our members, and the open source ecosystem are focused on ensuring training and certification opportunities are highly accessible to everyone who wants to seek them out."

I see this myself. I go to almost a dozen technology trade shows a year. And, whether they're open-source based, Open Source Summit or not, or CES, one thing is always true in the past few years: Companies aren't just hungry, they're starving for open-source and Linux-savvy workers. At some shows, especially ones about cloud technologies, such as Open Stack Summit, where literally every company was looking for employees with open-source skills.

This latest survey found that Linux skills are back on top as the most sought after skill, with 80 percent of hiring managers looking for tech professionals with Linux expertise. Don't have that much experience or certification? If you have some skills, 55 percent of employers are now offering to pay for a Linux certification, such as the entry-level CompTIA Linux+ to the mid-level Linux Professional Institute (LPI) LPIC-3: Linux Enterprise Professional Certification and the high-end Red Hat Certified Engineer (RHCE). That's up from 47 percent in 2017 and only 34 percent in 2016. When companies will pay for certifications, you know they're hungry for staff.

The eternal debate over the merit of certifications versus on-the-job experience continues as ever. But, according to Foote Partners, the average certification will get you a 7.6 percent premium over a job's base salary.

While Linux skills have become essential for entry-level tech jobs, other open-source technologies are gaining in popularity. Container expertise, for example, has exploded in importance. In 2017, only 27 percent with seeking that expertise. Today, 57 percent of hiring managers are looking for people who know how to handle containers.

Cloud technology experts are the second most sought after staffers at 64 percent. Security and web technologies come in next at 49 percent. Networking comes in at 46 percent.

And 34 percent of hiring managers are looking for professionals who know their way around open-source licensing and compliance issues. That's up from 29 percent last year.

Dice reports that open-source professionals with the most specialized and rarest skills can often write their own salary checks. That said, companies are increasingly finding other ways to overcome their companies' budget constraints for open-source workers overall. More than 70 percent now use incentives such as offering more vacation, flexible work hours. or telecommuting.

For open-source workers, it's not about salary or benefits. Only 13 percent of respondents reported that money and perks most influenced their decision to pursue an open-source career. Instead, they cited the ability to work with the latest technology, 65 percent; the freedom of open source 64 percent; and their personal passion about open source, 62 percent.

The fierce market for open-source talent shows no signs of abating. This is being driven by the push to DevOps and the use of cloud-based technologies such as containers and container orchestration.

Want to know more? The full 2018 Open Source Jobs Report is available to download for free. Go to www.linuxfoundation.org/open-source-jobs-report-2018.

Reported on the APCUG website (apcug2.org/penguin-platform/), and printed in Zdnet (https://zd.net/2M9DIIF).

Tidbits of probably useless information

It's illegal to drink beer out of a bucket while you're sitting on a curb in St. Louis!

No piece of square dry paper can be folded more than 7 times in half!

A group of geese on the ground is a gaggle, a group of geese in the air is a skein!

Over 2500 left handed people a year are killed from using products made for right handed people!

There are more than 10 million bricks in the Empire State Building!

If you counted 24 hours a day, it would take 31,688 years to reach one trillion!

* * * * * SOFTWARE and HARDWARE * * * * *

Ask Leo !

By Leo Notenboom, https://askleo.com/

Technology With Confidence

Making Technology Work For Everyone

Cryptomator: Encryption for Your Cloud Storage

Cryptomator is a powerful tool to protect the data you place into cloud storage.

I regularly hear concerns about using cloud storage — the biggest being that online files are at higher risk of compromise should your account or the storage be hacked. There are also concerns that your storage provider could be required to hand over your files to law enforcement agencies under certain circumstances. Those are all valid concerns. Cryptomator is a free encryption solution that addresses them.

Don't the providers encrypt?

Many online cloud storage providers do encrypt your data. The problem is that since they encrypted it, they can decrypt it. And while the folks at major online storage providers are professionals (with no interest in snooping around in your data), there have been rare instances of the so-called "rogue employee" poking around. The service providers also have the ability to turn your unencrypted data over to the authorities should that ever be required of them.

In addition, should *your* account be hacked, the data in your account would be available to the hacker in its unencrypted form, just as it's available to you. Provider-supplied encryption is nice, but it doesn't protect us as well as we'd like. The solution is simple: encrypt the data yourself. If *you* encrypt your data before it's uploaded to any online storage provider, you, and only you, control access to it.

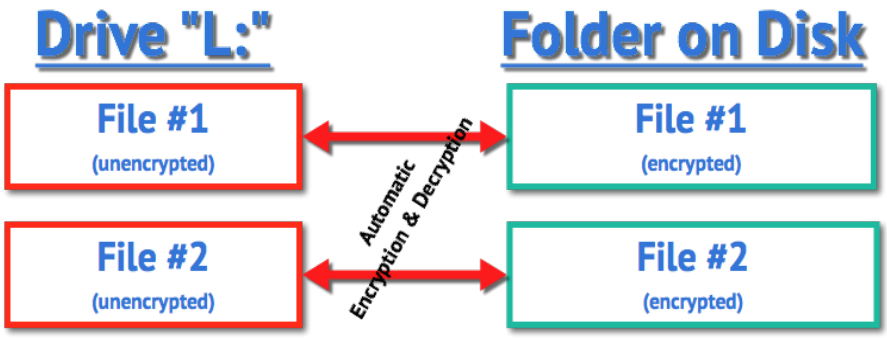
The hidden cost of doing your own encryption

There's one good reason *not* to encrypt your data yourself: web access. Unencrypted files are accessible via your service provider's web interface. Dropbox, as just one example, allows you to log in to your account from any machine and access the files stored in your account via the web. If you encrypt the data yourself, only encrypted data is available to you via a web interface. If you ever want to access your unencrypted data from another place — you can't.

The Cryptomator model

Cryptomator encrypts file-by-file, perfect for cloud storage providers like Dropbox, OneDrive, and others, that upload and download individual files as they change. You select a folder to be encrypted by Cryptomator, and assign it a passphrase to encrypt its contents. When you "mount" this folder using Cryptomator — providing the passphrase to do so — another drive letter appears, which I'll call L:. Anything written to drive L: is encrypted and written to the folder you specified. Anything read from that drive causes the corresponding encrypted file in the source folder to be read and decrypted on the fly. There's little, if any, noticeable impact on performance, since accessing the disk, not performing the encryption, is generally the slowest part of the operation.

The files in the original folder are always encrypted. It's only when the folder is mounted using Cryptomator that the files are visible in their decrypted form in the virtual drive.



An example of Cryptomator in use

Let's say I use OneDrive. On my machine, there's a folder:

C:\Users\leon\OneDrive

It contains all the files and folders that are part of my OneDrive cloud storage. I have many files and folders that automatically synchronize with the OneDrive servers, as well as all other machines on which I have OneDrive installed.

One of the folders in my OneDrive folder is:

C:\Users\leon\OneDrive\EncryptedFiles

I don't place any files in this folder directly. It starts out empty.

Next, I install Cryptomator and configure it to mount "C:\Users\leon\OneDrive\EncryptedFiles" as drive L:. I set up the passphrase required to mount it again in the future.

Drive L: appears on my machine.

I create a Word document on drive L:

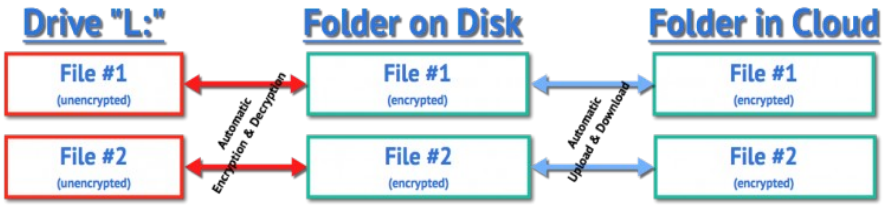
L:\MyPrivateInformation.docx

As soon as I save that document to drive L:, new files and folders appear within the EncryptedFiles folder:

C:\Users\leon\OneDrive\EncryptedFiles\d\2G\BQCY3SUZEVRU3MRAGLO6C62JGGGYZJ\5Y5RR6LM5SKSFZ6FIKULKNNBVQ3Y6DDTNGAKKX3VI2N72ZWM6KUOIGWL2AWCGB2TMY======

The file that was saved to L: was automatically encrypted and placed in the EncryptedFiles folder. This extremely obscure filename (along with others) is Cryptomator's encrypted version of my document. This is the only representation of the file that is written to disk.

Next, OneDrive notices a new file has appeared on disk. This *encrypted* file is then uploaded and distributed to all my machines running OneDrive. Note that only the *encrypted* version of the file has been uploaded.



I can continue to work on the file on L: to my heart's content. In a very real sense, it's just a file, and can be manipulated like any other. As changes are saved to disk, the corresponding encrypted version of the file is updated appropriately. Once I *dis*mount the EncryptedFiles folder, its corresponding drive, drive L:, disappears. The unencrypted versions of the files are no longer accessible. All that remains are the encrypted versions stored in the EncryptedFiles folder within the OneDrive folder, both online and on your hard drive.

It's for more than Windows

Cryptomator is available for:

- Windows
- Mac
- Linux

And there are also apps available for:

- Android
- iOS

That means you can continue to share your documents across all the platforms and devices supported by your online storage provider, but now you can easily encrypt the data you share.

What about BoxCryptor?

Long-time readers may remember a similar utility called BoxCryptor. I still recommend both BoxCryptor and Cryptomator; use whichever you feel most comfortable with. BoxCryptor is a commercial product. There's a free tier, which has some limitations, and paid tiers that provide more, including support. Cryptomator is free and open source, with no limitations on use. My bottom line is that Cryptomator is a convenient solution for making sure the data you place in cloud storage services remains secure and is accessible only by you.

I recommend it.

* * * * End of Article * * * *

Wi-Fi - 2.4 or 5GHz

By Carol Picard, Editor / Webmaster
Midland Computer Club, Michigan

I normally have acceptable network speeds throughout my house but one day, while downloading a file tomy desktop computer, which has a PCI wireless network card, I was only getting 3 Mbps download speed. This is my primary computer and is also located in a room farthest from where the router is located. My ISP is Charter Spectrum and highest download speed should be around 60Mbps.

Since slow speeds have happened before, I decided to take the time to see if there was anything I could do to improve the speed on the desktop computer. Running an Ethernet cable is an option but I was looking for a solution that would work for multiple devices, e.g., tablets, laptop computers, etc.

Using my laptop computer, I ran a speed test in several locations within the house. The speed test on the laptop computer in the same room as the Netgear R7000 router showed 60Mbps download speed. About 10 feet from router I was getting 30Mbps. At 20 feet from router it was 15Mbps but at the farthest distance (within the house) from the router it was 5Mbps. Speed tests normally fluctuate so I thought it was a good idea to run tests on different days and at different times of the day to get an average.

The router was dual band, capable of both 2.4GHz and 5GHz but had never used 5GHz.

I was surprised to discover that the PCI network card in seven-year-old desktop computer was dual band. I was concerned about the distance/obstructions between the computer and router. Several factors affect speed, other than distance, e.g., number and composition of walls, appliances, wiring, etc., and I had read that 5GHz had a shorter transmission distance than 2.4GHz.

After enabling the 5GHz band on the router, I ran more speed tests and was getting similar, high speeds on the laptop in the room where the router is located and on the desktop computer at the opposite end of house.

To check whether your computer is connecting at 2.4GHz or 5GHz, in Windows 10

- open Settings
- click Network & Internet Settings
- click Wi-Fi
- click Hardware Properties
- check information for Network band.

The Netgear R7000 router has a Smart Connect setting. The description of that setting indicates if SSID and network key are the same for both the 2.4GHz and 5GHz bands; the router would determine the best band for the connected devices. On the R7000, Smart Connect only applies to the main network. The Guest Network on the router has two bands (2.4GHz and 5GHz) but each band should have a unique SSID.

I configured SSID and network key on the router to enable Smart Connect. On the laptop, it successfully connected to the correct band, but using Smart Connect totally messed up the Internet connection on the desktop computer. I had difficulty connecting to the network and after connecting it either didn't get an Internet connection or got it for a short time and then dropped it. Resetting IP and flushing DNS on desktop computer didn't resolve problem. Neither did changing DNS servers. So, I reconfigured router to not use Smart Connect.

On the desktop computer, I ran various speed tests (beta.speedtest.net):

1. 5GHz band and results showed Download = 67.67 Mbps; Upload = 5.71 Mbps.
2. 2.4GHz band results showed Download = 35.91Mbps; Upload = 5.71 Mbps.

I also tested using Charter Spectrum speed test.

- 5GHz band results showed Download = 66.40 Mbps; Upload = 5.75 Mbps.
- 2.4GHz band results showed Download = 39.42Mbps; Upload = 5.97 Mbps.

Upload speeds are almost always considerably slower than download.

Normally, when working on a specific problem, I find one or two more problems but this time, while working on a solution for the Internet speed problem at home, I discovered a solution to another problem. We recently changed the location for our Club meetings and when attempting to connect to the Internet at the new location, several members did not see the wireless connection on their devices when viewing available networks and were unable to connect to the Internet.

While testing different devices at home, e.g., laptop computers and tablets, I noticed that some of the devices were not showing the 5GHz SSID. I checked specifications for those devices and found the internal network card only had single band, 2.4GHz capability. A device that only has 2.4GHz network card, cannot see a network broadcasting at 5GHz. To further test this, purchased a Netgear AC1200 Wi-Fi USB Dual Band Adapter. Using the AC1200 adapter I could bypass the internal 2.4GHz network card and connect to the router's 5GHz band. I further tested this at last month's computer club meeting and was able to connect to 5GHz at the meeting location.

There are different ways to determine if a network card/adapter is capable of dual band. Under Device Manager, Network Adapters, description may indicate whether it is dual band.

In Windows 10

- open Settings
- click Network & Internet
- click Status
- click View your network properties
- scroll down to Wireless Network Connection

You can also try an Internet search for the model number of your device; specifications may show information Security reminder: If you own your own router make sure you have changed the password for logging into the router (this is not the same as the SSID password for connecting devices to the network/Internet). Also check for and install router firmware updates, especially security updates.

From the September 2017 issue of Bits and Bytes, capmidmi@yahoo.com, mcc.apcug.org.

Mobile Highway

Items of interest to Mobile Device Users

One Dongle to Rule Them and In the Darkness, Bind Them

By Chris Woods
Under the Computer Hood UG

When you get a wireless mouse, keyboard or any other of a myriad of wireless devices,

what is common is that they all come with their own dongle. Most operate within the 2.4 GHz range and are mated to that device. Lose the dongle and you might as well kiss it goodbye. Ever noticed, on some of these devices, a tiny orange asterisk tattooed upon its surface?

The orange asterisk symbol stands for Unifying Receiver, one of the dirty little secrets of peripheral manufacturers. Why have all your USB ports taken up with dongles when only one is required, the Unifying Receiver?

Logitech introduced its Unifying Receiver back in 2009. At first, it was only for Logitech's line of devices, and it was limited to keyboards and mice. Many manufacturers have quietly included the same function on their peripherals. One of the pieces that make this magic work is the Logitech Unifying Software (http://support.logitech.com/en_us/software/unifying).

The software acts the same as a Bluetooth pairing, mating the device to the receiver. To set up this paring you first download the software. Then plug in the Unifying Receiver to a USB port and allow its driver to load. Finally, you run the software. When you run the software, there is a prompt that will ask you to turn each device (mouse, keyboard, etc.) off and on. If the device is compatible it is paired to that one receiver. To add other devices later you run the software again and follow the prompts. Right now, it's still limited to six devices per receiver. A space saver for systems that are port limited, provided the device is recognized as compatible. As of this writing, according to Toms Hardware: "A Logitech Receiver will pair up to 6 Logitech and non-Logitech peripherals, provided they both have the symbol. A Microsoft Receiver will pair most devices...but not Logitech."

I have not seen any compatibility lists, but I can confirm from a tech standpoint that most peripherals that have the symbol pair without issue. I have a user at work that has a Logitech Unifying Receiver with an Asus keyboard, a Logitech mouse, and a Wacom drawing tablet. The limiting factor seems to be if your OS sees the device as an HID (Human Interface Device). For someone using many wired HID's and wanting to switch to wireless to open USB ports the Unifying Receiver can come in very handy.

From the February 2018 issue, Drive Light, www.uchug.org, 1editor101@uchug.org.

Nothing Bad Ever Happens

By Greg Skalka, President
Under the Computer Hood User Group, CA

Nothing bad ever happens to me
Nothing bad ever happens to me
Why should I care?
(Lyrics by Danny Elfman, from the 1983 Oingo Boingo song *Nothing Bad Ever Happens*)

As far as technology goes, I've been pretty lucky. I've had very few things fail in the nearly 40 years I've been playing with computers and other tech devices. Sure, there are a few things here and there that break now and then, but overall, the technology that I've bought over the years has been very reliable. It seems nothing really bad ever happens to my tech.

I took note of this reliability in my tech stuff when I realized recently that I do have a lot of old devices around, many that I still use (or at least can still use). I can't name too many items I've seen fail over the years, and certainly can't think of any that have been catastrophic failures. Sure, I've bought a few items that were DOA (dead

on arrival), but I don't count those, as I was able to return them under warranty. If an expensive tech purchase had failed not long after the warranty expired, then that might be a disaster, but I don't recall that ever happening to me. I do remember buying a netbook (remember those small laptops, kind of a precursor to a Chromebook?) in 2009 and found the display had problems from the first time I turned it on. I just sent it right back to Amazon and received another one that worked fine for many years (or at least as well as these underpowered laptops ever did), and probably still works to this day.

I say that the netbook probably still works to this day because I must admit, that although I do still have it, I have not tried to use it in many years. That is often one thing that technology items have going for them in trying to last - we often lose interest in them well before they would have failed. The netbook was running up to 2014, as my hard drive backup records show the last backup for that computer was on 4/21/14, right after the last update that was available for Windows XP. I'm pretty sure I've not used it since then, as I've bought many newer and more capable computers to replace it.

In spite of how well current devices may be made, my good luck with technology probably does not come as inevitable or by chance. I try to take good care of my equipment, as not only does it often constitute a significant financial investment, it also represents an important resource to me, that I don't want to be without due to failures.

I try to use care with all my tech items but am particularly insistent on maintenance and preventative measures on those items I find most critical in my daily life. I take great care in handling my portable electronics, more so than I often see from other users. My laptops and Chromebook are always transported in a padded case; I have my smart phone completely surrounded by screen protection and a shock-resistant case. I keep the air vents clean and the fans running on my computers. I do a reasonable job of keeping my computer data backed up (I have not so far lost anything of significance). Surge protectors and UPS (uninterruptable power supply) units protect my most critical and expensive tech devices.

I perform my own auto maintenance and repairs, both to save money and make sure it is done right. This does mean I do have to learn how, but this knowledge provides additional benefits when having to diagnose problems on the road. Not everything may be perfect with some of my cars, but they get me where I need to go. I didn't bother fixing the back-up sensors on my wife's car when it got older, as I felt it was not worth the cost and effort. At some point she got a new car, and I inherited the old one, which at 226k miles and 13 years old is still my daily ride.

There are a few minor tech items that I would not count in the failed column as they really never performed up to expectations from the start. I wanted to experiment with network security cameras a few years ago and bought some cheap ones ($25). These never really worked well for me; they were difficult to set up and to keep connected to my home network. I finally gave them to my son and bought a more reputable and expensive brand, which have worked well.

I fear there are some tech devices that may be designed by the manufacturer to be disposable. Apple products may be designed that way, but are too expensive to be disposed frequently, so I avoid them. I often try to fix our broken home appliances, but my wife's track record with floor cleaning devices is not too good. It seems we need a new small vacuum or steam mop every few years, and these don't seem to be repairable, though at least the ones she picks are not that expensive.

Here is a bit of a run-down of my tech reliability over time by category; see how it compares to your own.

Computers - I don't know how many computing devices I've had since that Timex Sinclair 1000 I bought in 1982; it could be in the 20's. I've had several PC-XT clones, many tower cases running everything from DOS through every version of Windows up to 10 (but I've never had Microsoft Bob) and six laptops. I am actually writing this on my oldest running computer, a tower case with a Pentium 4 processor and Windows XP (and not connected to my home network). It has been running almost continuously since 2005, with no failures that I recall.

When we had kids at home, we had four desktop PCs running in our house. Now the two of us that remain regularly run three desktops, two laptops and a Chromebook. Over all this time I've never had a motherboard fail, don't recall ever having a memory module fail, and only had a couple of hard drive failures. I can't remember when the last hard drive failure happened; it has been so long ago. None of my running drives are that old, however; I've upgraded the drives in our two laptops twice in the last six years (once to larger drives, and again to hybrid drives). I bought a few spare PATA hard drives as spares when SATA became more prevalent; now that XP computer is my only one that can use them. I don't recall ever having a computer power supply fail; that spare I bought ten or more years ago 'just in case' is now probably obsolete. Surprisingly, I've never had a fan fail.

Computer Accessories - I have bought a bunch of external USB hard drives for backup and data storage over the

years and have never had one fail. I did have some regularly-used small encrypted USB hard drives that did fail after many years; the cable connector to the drive wore out and became unreliable. By that time, however, larger sized drives were needed anyway. USB Flash drives are supposed to wear out, as each memory location is rated for a limited number of writes. Even with Flash drives that I tend to use a lot, I've never seen any evidence of failure, as I again tend to keep moving up to larger sized devices anyway. I have had a couple of wireless mice fail, but they are inexpensive. Keyboards seem to be unbreakable.

Network Products - I did have one router failure about ten years ago, but I had a cheap spare on hand to use temporarily until I bought a good replacement. Now it is sitting unpowered, as I'm using the router built into my AT&T U-verse modem. I think I had an Ethernet switch fail many years ago. Most of my switches now are fairly new, as I've been trading them up to 8-port and/or Gigabit. I've had four network hard drives, but their size generally becomes insignificant over time and I then shut them off, rather than see them fail. I did have a 120G network drive fail, and I may have a 500G that had issues recently (I have not yet had time to diagnose it). No data has been lost, however, as I back these up too.

Mobile Phones - I've had my current Samsung Android smart phone for less than a year - so far, so good. My previous phone was a Samsung slide 'feature' phone that could text but not access the Internet. When its camera failed, it was probably a blessing, as it got me to finally graduate to a smart phone; it worked otherwise. My phone before that was a dumb flip phone which worked fine, but I abandoned it when I switched to being on my wife's cell plan.

Cameras - I have owned many digital cameras over the years, from a 2 Megapixel Olympus in 2001 to my 18 MP Panasonic today. In almost all cases, I got a new one because image resolution went up and camera prices went down, not because my old one broke. I did have one major fail that was all my fault. I dropped my old Panasonic 16 MP camera at the Long Beach Grand Prix two years ago and cracked the rear display screen. I soldiered on with it, using the viewfinder display, until the flash also failed, and my wife gave me the new one for my birthday last year.

Overall, my tech success has been pretty positive. I've been careful in picking devices to buy, and I've tried to take care of them as best I could. I have been rewarded by years of reliable use with very few failures. I don't look at my positive results as a reason to abandon my practices of care and backups, but rather a justification for them. I hear enough of others having grief with tech failures to know that things can and do break. I've seen others casually handling or flipping their phones (no wonder their screens have cracks), not shutting down computers correctly and disconnecting devices by yanking on the cables. No wonder it seems (at least relatively speaking) that nothing bad ever happens to me.

From the March 2018 issue, Drive Light, www.uchug.org / president@uchug.org.