Newsletter of the North Orange County Computer Club

range Bytes

Volume 46 No 10 **October 2022** **$1.50**

NOCCC meetings for Sunday November 6, 2022

MAIN MEETING -

.Presentation for Main Meeting will be optional.
An open meeting where members interact about computer stuff they like.
Or a computer program presentation by your President. Your choice.

Special Interest Groups (SIGs) & Main Meeting Schedule

9:00 AM – 10:30 AM

Beginners Digital Photography ....Science 129
Questions and Answers about Digital Photography

Linux for Desktop Users……………….Science 131
Beginners' Questions about Linux

10:30 AM – 12:00 PM Noon

3D Printing .... Irvine Auditorium
Questions and Answers about 3D printing

Advanced Digital Photography… ....Science 129
Questions and Answers about Digital Photography

Linux Administration ....Science 131
More topics about the Linux operating system

Mobile Computing ....Science 109
We discuss smartphones, tablets, laptops, operating systems and computer related news.

VBA and Microsoft Access/Excel........Science 127
Using VBA code to enhance the capabilities of Access and Excel

12:00 PM Noon – 1:00 PM

3D Printing………………………………. Irvine Auditorium
Questions and Answers about 3D printing

PIG SIG ……………………………………. Irvine Courtyard
Bring your lunch. Consume it in the open-air benches in front of the Irvine Hall. Talk about your computer and life experiences.

1:00 PM – 3:00 PM Main Meeting

See above

…………..……. Irvine Auditorium

3:00 PM – 4:00 PM

Board Meeting……………………………………………
Science 129

Verify your membership renewal information by checking your address label on the last page

Mark your calendars for these meeting dates
2022: Nov 6, Dec 4,
2023: Jan 8, Feb 5, Mar 5, Apr 2, May 7,

Coffee, cookies and donuts are available during the day in the Irvine Hall lobby.
Food and drinks need to remain outside the Irvine Auditorium.

"Friends Helping Friends"
since April 1976

Table of Contents

Special email addresses
Jim Sanders is editor@noccc.org
membership@noccc.org

Our Website
WWW.NOCCC.ORG

Reminder: Membership expiration dates have been advanced by two years. So if your membership expired in August, 2020 it was now August, 2022. Or to put it another way, your membership renewal is now past due. The same concept holds true for Sept., so pay your renewal at the meeting.

The main meeting was lightly attended but the presentation was informative. There were not enough officers present for a quorum, so a meeting was not held

Board of Directors

Contact information and email forwarding addresses

President Robert Strain
president@noccc.org **(cell 714.222.2140)**

Vice President (acting) Jim Sanders
vicepresident@noccc.org **(714-544-3589)**

Secretary position is open
secretary@noccc.org

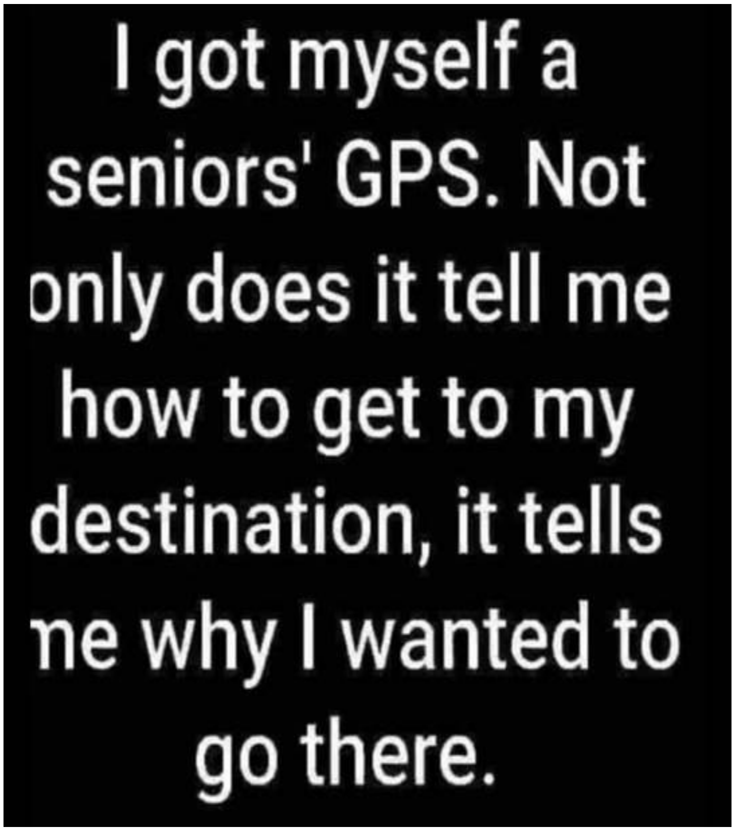
Treasurer Dr. Don Armstrong
treasurer@noccc.org **(home 714.773.1187)**

Webmaster Jim Sanders
webmaster@noccc.org **(home 714.544.3589)**

Director Terry Dickson
terry@noccc.org **(home 714.899.9913)**

Director Dennis Martin
dennis@noccc.org **(home 951.926.3065)**

Director Richard Miller
richard@noccc.org **(cell 714.309.1504)**



I got myself a seniors' GPS. Not only does it tell me how to get to my destination, it tells me why I wanted to go there.

Online Privacy Is a Myth:

What You Can and Can’t Do About
It by Chris Hoffman, EditorinChief of HowTo Geek
We all want to recover (and maintain) our online privacy. There are lots of features and industries built around fighting for privacy, from privatebrowsing modes and tracker blockers to private VPNs. But online privacy is a myth—and offline privacy might be one, too.

Yes, a Myth

Myths are stories (or narratives) that are often foundational to a society’s beliefs. The myth of online privacy is like that: Privacy feels foundational in our society. To the extent we accept we don’t have privacy online, it feels like something we’ve lost—something that we can perhaps recover with the right software tweaks, behaviors, or perhaps regulations. When you think about it, the myth of online privacy is even beneficial to those industries that benefit from the lack of it. We all might agree that there’s no privacy online, but leave us to a search engine, and we’ll search an endless list of everything that comes into our minds, including potentially sensitive topics like medical questions. Police even dig through those search histories to look for criminals.

Breaking the Privacy Illusion

We may all agree that online privacy isn’t something we have. But do you realize how little privacy you actually have? First of all, when you go online, your Internet service provider— whether that’s a home Internet connection or a cellular data connection — can see all the websites you’re accessing. In the USA, they can even sell your browsing data. Your mobile carrier may even be tracking and selling your app usage activity. When you visit a website, it can see your IP address and use that to track you across visits. But it likely loads a lot of tracking scripts, too. Those tracker networks can track your activity across multiple websites. That’s one reason you see shopping ads chase you across the web after you look up a particular product. Even if you’re clearing cookies, there are a lot of ways to fingerprint your web browser. “The cloud” is just someone else’s computer. If you upload your files to the cloud without using endtoend encryption—something most services don’t offer—your files can be viewed and accessed by the company that owns the cloud service. The same goes for messages and emails, which generally aren’t encrypted either. Okay, you might know all that—but did you know that advertisers can tie your instore purchases and visits back to ads you see? For example, Google has a product that does this, and one of the data sources it uses is the nebulous “transaction data uploaded by the advertiser or aggregated and anonymized data from third parties.” Your credit card usage is being used to track you, too. Did you know that Facebook’s advertising tools are so granular that you can target ads so narrowly that you can show them to only one individual? Government surveillance is a given: Edward Snowden famously drew attention to massive warrantless government surveillance of Internet and phone data. The NSA’s XKeyScore software reportedly allows realtime search and access to the massive amount of data being logged about online activity. The online world isn’t something completely separate from the real, physical world, of course. The USA is full of automatic license plate readers, and many of them are now linked together in a big network. Even if you get off the computer and go for a drive, your movements are being tracked and logged. Amazon may be handing videos from your Ring doorbell camera over to the authorities without your explicit consent. Your cell phone location data is being used to track you, too.

What Can You Even Do?

An article like this one could go on and on with examples. Do a little digging, and you can find many more examples. The amount of data being collected, crunched, and analyzed about us at all times is tough to conceptualize. There are no perfect fixes. Private browsing will stop your browser from remembering your history and give you a fresh set of temporary cookies, but your IP address is still out there. You can avoid using Facebook, but Facebook has a shadow profile on you anyway. You can use a VPN, but you’re going to sign into something eventually—which will tie your identity to your browsing in the VPN—and you’re placing your trust in a VPN that hopefully doesn’t keep logs. So what can you do? Well, you can still make a dent in it. If you’re currently broadcasting your life as a 24/7 live stream, turning off the camera means less data is out there. You can use a VPN along with private browsing mode to disguise your browsing—but don’t just rely on a VPN alone, and understand that you’re trusting the VPN. You could use Tor—though there have been vulnerabilities in Tor, too. You can use more private, encrypted services —for example, chatting on Signal instead of plainold SMS messages. You can keep your sensitive files more private, storing them locally or securely encrypting them before uploading them to online storage.And yes, you can go further: Using cash, for example, and putting together facial accessories that will stop facial recognition cameras.

What’s the Point? Threat Modeling 101

But as you’re sitting there using Tor on a computer running Tails trying to figure out how to go off the grid without actually going off the grid, you might want to ask yourself: What’s the point? No, we don’t mean give up—we mean consider what you’re actually defending against. • You might not care if Facebook realizes you’re interested in seeing the latest movie. But you might want to fire up that VPN and private browsing mode when you’re searching for information about a medical issue. • You might be fine with storing photos of your vacation unencrypted in the cloud, but you might want to keep sensitive financial documents more secure. • You might be fine chatting with your plumber over SMS, but you might want to have a private conversation with your spouse on Signal. It’s all about your threat model—what are you actually trying to defend against? Once you know what you care about keeping private, you can take steps to keep that individual sensitive thing private rather than be overwhelmed with all the data collection going on all the time. Unfortunately, that’s not a recipe for “online privacy.” There’s no easy way to flip a privacy switch and regain a mythical state of privacy. But there are things you can do to better shield specific things and keep them more private. This article was copied from https://www.howtogeek.com/819686/onlineprivacyisamythwhatyoucanandcantdoaboutit/

North Orange County Computer ClubDr.
Donald Armstrong
709 Rosarita Drive
Fullerton, CA 92653

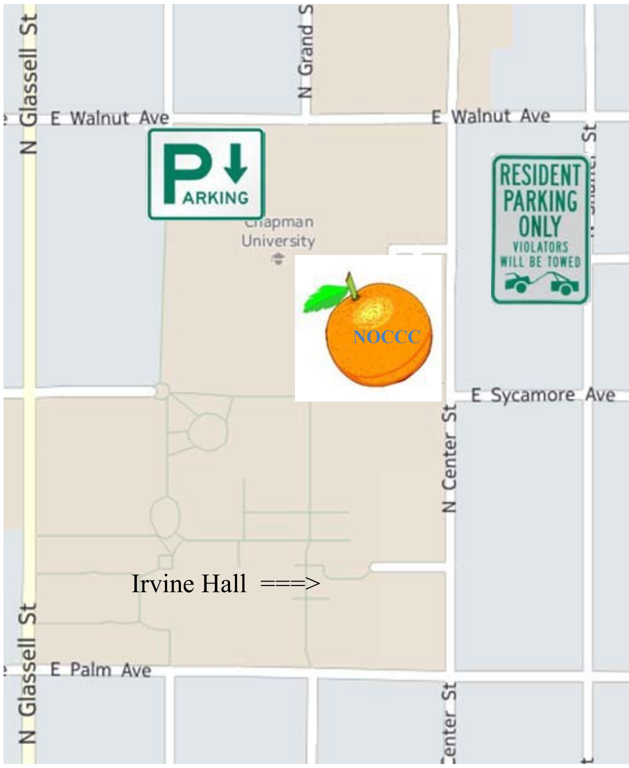
To All Members:

The line above your mailing address now shows your joindate. Please use your join month to choose when to renew your membership.

Dated Material – Please deliver before November 6, 2022

Membership Level ($)	1 Year	3 Years
Individual Member	35	90
Each Additional Family Member	15	40
Full-Time* Enrolled College Student	20	
Enrolled High School Student	15	
*Minimum 12 Semester Hours		
Business Member + Ad (Business Card)	180	
Business Member + Ad (¼ Page, ½ Page)	465,	800
Business Member + Ad (Full Page)	1,475	
Contributing Member	75	
Supporting Member	100	
Advocate Member	250	
Patron Member	500	

Directions to the NOCCC meeting location



An International Association of Technology & Computer User Groups

Enter CA-55 N (Costa Mesa Freeway) crossing Interstate 5 toward Anaheim/Riverside for 9 miles. *Notice freeway and street signs stating "Chapman University."* Exit toward E Chapman Ave. Turn right onto N Tustin St. Turn left onto E Walnut Ave.

1) Turn left past N. Center St. for the **best place to park** in the underground parking structure (Lastinger under the sports field).Pay the small fee ($2) to park Ask members or help@noccc.org about parking details, restrictions, and our price break!

2) Turn left onto N Center St. On the right is the Hashinger Science Center, 346 N Center St. Orange California. Parking on the University side is free. Parking on the residential side is a city violation that may cost you a tow away and a ticket!