

The PCLinuxOS magazine

Volume 220

May, 2025



ICYMI: New Runway Safety Measures Coming To An Airport Near You

How To Select A VPN Provider

Setup Your VPN's Servers Easily In NetworkManager

*GIMP Tutorial:
Create A Word Art Logo*

*Tip Top Tips: Fixing
Filesystems Automatically
After System Crash/Reset*

Wiki Pick: Numlock On At Login

Typst Cookbook: Part One

How To Delete Your 23andMe Data

PCLinuxOS Puzzled Partitions

And more inside...

In This Issue...

- 3 From The Chief Editor's Desk**
- 4 Screenshot Showcase**
- 5 PCLinuxOS Recipe Corner:**
Maple Glazed Bacon Chicken Bites
- 6 How To Select A VPN Provider**
- 9 Screenshot Showcase**
- 10 Typst Cookbook: Part One**
- 17 Screenshot Showcase**
- 18 How Do You Solve A Problem Like Google Search?**
Courts Must Enable Competition While Protecting Privacy
- 20 Screenshot Showcase**
- 21 Setup Your VPN's Servers Easily In NetworkManager**
- 26 GIMP Tutorial: Create A Word Art Logo**
- 28 Privacy On The Map:**
How States Are Fighting Location Surveillance
- 32 Screenshot Showcase**
- 33 ICYMI: New Runway Safety Measures Coming**
To An Airport Near You
- 42 Tip Top Tips: Fixing Filesystems Automatically**
After System Crash/Reset
- 43 Screenshot Showcase**
- 44 Wiki Pick: Numlock On At Login**
- 45 How To Delete Your 23andMe Data**
- 47 PCLinuxOS Recipe Corner Bonus:**
French Onion Beef and Noodles
- 48 PCLinuxOS Puzzled Partitions**
- 52 More Screenshot Showcase**

The **PCLinuxOS** magazine

The PCLinuxOS name, logo and colors are the trademark of Texstar. **The PCLinuxOS Magazine** is a monthly online publication containing PCLinuxOS-related materials. It is published primarily for members of the PCLinuxOS community. The magazine staff is comprised of volunteers from the PCLinuxOS community.

Visit us online at <https://pclosmag.com>.

This release was made possible by the following volunteers:

Chief Editor: Paul Arnote (parnote)

Assistant Editor: Meemaw

Artwork: Paul Arnote, Meemaw

PDF Layout: Paul Arnote, Meemaw

HTML Layout: tbs, horusfalcon

Staff:

YouCanToo

David Pardue

Alessandro Ebersol

Contributors:

The PCLinuxOS Magazine is released under the Creative Commons Attribution-NonCommercial-Share-Alike 3.0 Unported license.

Some rights are reserved. Copyright © 2024.



From The Chief Editor's Desk

If you're a Linux user, your time to **rejoice** is close at hand.

See, starting October 14, 2025, Microsoft is shutting down support for Windows 10. According to an [article](#) from Forbes, Microsoft is preparing millions of PC owners for the unprecedented device cliff edge that hits on October 14, when support for Windows 10 ends. As reported by [Windows Latest](#), the company is now telling users to stop using those devices and to “recycle Windows 10 PCs” that “can’t upgrade to Windows 11.”

That last sentence is what makes my heart smile. That means Linux users should get ready to “recycle” (as in repurpose) old, decrepit Windows 10 computers into powerhouse computers running Linux (hopefully, PCLinuxOS). Most of those computers being “obsoleted” by Microsoft are not only fully capable of running Linux, but many of them are gently used, with LOTS of life remaining in them. Finally, those computers can live out the rest of their technological lives free from the worry of misapplied Windows Updates, and free from the worry of viruses and many other pieces of malware. Some might even contend that Windows itself IS the biggest piece of malware ever devised.

Keep your eyes peeled. You're likely to see a flood of computers hit the resell market for cheap. Check out your favorite refurbishers.



Check out your swap-and-shops. Check out your thrift stores. I have a feeling that there will be a LOT of gently used computers finding their way to Linux users for cheap. And, don't discount what could be the best buy of all, by curbside shopping ... especially in more affluent neighborhoods.

So, how do I already know that these computers will go for cheap prices? It's simple economics. Supply and demand. The supply of gently used computers will soon explode. There will soon be a flood of these computers that aren't capable of running Windows 11, and any time that happens, Linux users can literally clean up.

A lot of these computers have fairly recent processors, good amounts of RAM, and fairly roomy storage drives. And, many of those drives are solid state drives, instead of spinning rust drives.

Microsoft, on their “support” [page](#), wants you to scrap your Windows 10 computer. As in, send it to the landfill. And then, they want you to buy a new computer capable of running Windows 11. Of course, what they fail to mention is that you can also install a different operating system (hello Linux!) on those computers.

After all, that is what drove me to Linux. The last version of Windows that I routinely ran was Windows XP. The transition from XP to Vista is what pushed me to Linux. I had just bought my first laptop computer less than a year before the release of Vista, and it didn’t have the hardware specs to run Vista. Despite that, I knew there was a LOT more life left in that computer. So, I started looking for alternatives, since Windows XP support was coming to an end. I was correct. I ran PCLinuxOS on that particular laptop for another three-plus years.

The situation now with Windows 10 support ending is remarkably similar to what I experienced all those years ago with the transition from Windows XP to Vista. Back then, you could get a used laptop that wasn’t capable of running Vista for dirt cheap ... if not for free. I suspect history will repeat itself with this latest push by Microsoft.

I know that Linux users “love” for Microsoft is pretty lopsided, well-earned, and justified. But

don’t look a gift horse in the mouth. Keep your eyes peeled for some quality, useful hardware available for a very cheap price. Do expect a flood of those hardware components the closer we get to October 14.

This month’s cover was created by me, to signify the annual arrival of the spring storms that frequent my area when Spring finally

arrives. I just figured I’d put a PCLinuxOS twist on the image while I was creating it. My GIMP skills are nowhere close to Meemaw’s, but every once in a while, I can figure out how to create a really nice image.

Until next month, I bid you peace, happiness, serenity, prosperity, and continued good health.

Screenshot Showcase



Posted by The CrankyZombie, on April 1, 2025, running KDE.

PCLinuxOS Recipe Corner



Maple Glazed Bacon Chicken Bites

Serves: 6

INGREDIENTS:

1 lb chicken breast, cut into bite-sized pieces
8 slices of bacon, cut in half
1/2 cup maple syrup
1 teaspoon garlic powder
1/2 teaspoon black pepper
1/2 teaspoon salt
1 tablespoon olive oil
Toothpicks for skewering

DIRECTIONS:

Preheat the Oven:

Preheat your oven to 400°F (200°C). Line a baking sheet with parchment paper for easy cleanup.

Prepare the Chicken Bites:

In a large bowl, combine the chicken pieces,

garlic powder, black pepper, and salt. Toss until the chicken is evenly coated.

Wrap with Bacon:

Take a half slice of bacon and wrap it around each piece of chicken. Secure the bacon in place with a toothpick.

Glaze with Maple Syrup:

In a small bowl, mix the maple syrup with the olive oil. Brush the mixture over each bacon-wrapped chicken bite.

Bake:

Place the bacon-wrapped chicken bites on the prepared baking sheet. Bake in the preheated oven for 20-25 minutes, or until the bacon is crispy and the chicken is cooked through.

Serve:

Serve the Maple Glazed Bacon Chicken Bites hot. They make a perfect appetizer or party snack that everyone will love!

NUTRITION:

Calories: 122 Carbs: 1g Sodium: 434mg
Fiber: 0g Protein: 16g

**Looking for an old article?
Can't find what you want?
Try the PCLinuxOS
Magazine's searchable
index!**

The **PCLinuxOS** magazine



How To Select A VPN Provider

by Paul Arnote (parnote)

So you've decided to use a VPN to enhance your online privacy and security. But looking around at the VPN landscape, it can be quite overwhelming to know which VPN provider to choose or go with, given how many there are out there.

What do you need to look for? Certainly, the added cost of using a paid VPN provider comes into play, but cost isn't the most important thing to consider, believe it or not. What we'll try to do here is to shine some light on many of the more daunting aspects involved in selecting a VPN provider.

By the time you're considering using a VPN, you should already have an idea of how VPNs work. If you don't know this information already, you're (in essence) putting the cart in front of the horse. In that case, you need to undertake a little self-education, and that is way beyond the scope of this article. There are plenty of articles in a wide assortment of media outlets that already do an excellent job of explaining how a VPN works.

In the interest of full transparency, I have been a regular user of a VPN provider for over the past eight years. I use Private Internet Access (a.k.a. PIA), but in no way should that be construed as an endorsement of just them. For me, they just

"checked all the boxes" for what I was looking for in a VPN provider. I urge you to do your own research, and come to your own conclusions about which VPN provider best serves your needs.



Image by [Stefan Coders](#) from [Pixabay](#)

Most Important: Log Policy

You will want to choose a VPN provider that does NOT keep user logs. Those user logs could contain your originating IP address, who you connect to with your VPN, your location, and a whole host of other revealing information that infringes on your privacy. And, we're not even talking about whether you're doing illegal or questionable actions while online.

Even if you're not doing anything illegal or questionable, the "no logs" policy of your VPN provider protects you from unreasonable searches or suspicions by authorities. I do not subscribe to the "I've-done-nothing-wrong-so-I-have-nothing-to-worry-about" school of

thought. Instead, I have a reasonable expectation of privacy regarding what I do, where I go, and who I interact with in my "online travels."

Of course, if your chosen VPN provider keeps no logs, there's nothing to share or turn over when the "authorities" come knocking. Even better yet are VPN providers who operate RAM-only VPN servers. That means that NO data is saved to a hard drive, ever, for any reason. Most reputable top-tier VPN providers have a "no logs" policy. If the VPN provider you're considering signing up with doesn't, keep looking for one that does.

In the past, there have been VPN providers who professed a "no logs" policy, but then they were discovered to have actually kept logs. For what it's worth, those VPN providers are no longer in business. Today, saying you don't keep logs when you actually do keep logs is the express way to commit corporate suicide in the VPN provider business. People concerned about their privacy simply will not patronize or tolerate a VPN provider who acts like a proverbial snake-in-the-grass, and take their business elsewhere.

Keep in mind that nearly all of the "free" VPN providers (they are out there) DO keep logs, so your information is readily available to the authorities for the asking. While it may seem a bit trite and worn out, the old adage "you get what you pay for" is apropos in describing the "free VPN providers."

VPN Provider Costs

The next thing to wonder/worry about is the costs associated with a top-tier VPN provider. It's important to remember that the longer term you sign up and pay for with a top-tier VPN provider, the cheaper the "per-month" cost will be.

Let's look at NordVPN as an example. For a one-month price for NordVPN, expect to pay \$13.99 (prices current at the time that this article was written). But, if you switch to a 2-year plan (and they provide three free extra months when you select the 2-year plan), that price is \$107.33, which comes out to \$3.99 per month. Similarly, PIA (the VPN provider I use) charges \$11.95 on a month-to-month plan, but also offers a three-year plan. Under that three-year plan, you get 40 months (three years plus 4 extra "free" months) for \$79. That brings the price to only \$1.98 per month. Most of the top-tier VPN providers offer incentives like this for paying for an extended service plan.



Image by [Dan Nelson](#) from [Pixabay](#)

Encryption

One of the key features about using a VPN is that the data from your computer to your VPN provider's server(s) is encrypted. Your ISP can see traffic, but (thanks to the encryption) they cannot see what you are doing. There is a use case where this is not the case (DNS leaks), but even that is easy enough to eliminate. I discuss this problem fully in my companion article elsewhere in this issue about how to set up your VPN servers in NetworkManager, so I refer you to that particular article, rather than rehashing it all again here.

During most of the time I've spent with PIA, I've used their OpenVPN files to connect. For a brief period when I first signed up with them, I used their dedicated app to connect to their VPN service. But, I find that the OpenVPN files provided just as much protection as their dedicated app did. Keep in mind that you may not be able to "find" the OpenVPN files to download until you log into the VPN provider's website, and logins are restricted to paying customers.

When selecting your encryption level, I would recommend using the strongest encryption available (or that you can use). For example, PIA has two sets of OpenVPN files (via TCP) to choose from. The first one uses 128-bit AES (Advanced Encryption Standard) encryption, while the TCP (Strong) OpenVPN files use 256-bit AES encryption. Do you want to guess which one I use? AES encryption is recognized as the worldwide standard for solid cybersecurity, and

you'll frequently see it described by VPN providers as being "military-grade."

When you connect to a VPN server, two things happen: the VPN encrypts your connection and reroutes your traffic through a server in its network. This hides your real IP address behind one from whichever location you're connected to. All your traffic passes through the VPN server before reaching the website you're visiting. This means the website can only see the new VPN server's IP address, not your actual IP address. Since your traffic is encrypted, outsiders can't snoop on your activity either. This is why VPN servers are so unique. They change your location, but they also secure your activity.

Where Is Your VPN Provider Located?

Where your VPN provider is located can be an important consideration. You can expect to have greater privacy and security when your VPN provider is located/based in a country outside of the "Five Eyes" countries. The Five Eyes countries are Australia, Canada, New Zealand, the United Kingdom, and the United States. This alliance focuses on intelligence sharing and cooperation, particularly in signals intelligence.

For example, NordVPN is based in Panama, which is known as one of the "privacy haven nations." ExpressVPN is based in the British Virgin Islands (another "privacy haven" nation). Malaysia is another "privacy haven" nation.

Even though PIA is based in the U.S., their “no-logs” policy leaves nothing to hand over to law enforcement authorities, which makes their physical location inconsequential.

Since I’m a PIA user, I’ll keep referring back to them because that’s what I’m most familiar with. PIA has servers located in all 50 states in the U.S., as well as many, many other countries across the globe. Some countries, like Canada, the U.S., the U.K., Australia, and Germany have multiple servers available. PIA has servers located in 91 different countries. And even though I haven’t “updated” my PIA OpenVPN files in quite some time, I have a hundred different servers listed in my “collection” of OpenVPN files, located in countries all over the world. Some VPN providers boast about having something like 2,000 servers. Just keep in mind that it costs money to keep all of those servers online, updated, and running, so that cost burden may be reflected in the price you have to pay.



Image by [Süleyman Akbulut](#) from [Pixabay](#)

Does The VPN Provider Suit Your Use?

On its face, this question sounds a bit odd. But let’s look at this objectively.

Some sites don’t like for you to connect to them while using a VPN. As such, they’ll often display an error when you attempt to connect to them while you’re connected to your VPN. Netflix is notorious for this, as are other sites like Amazon Prime, Disney+, and BBC iPlayer. Many of the top-tier VPN providers have unlocked access to streaming from popular sites. If your need includes streaming from popular streaming sites, you’ll most likely want to restrict your search to those top-tier VPN providers who have unlocked access to the most popular streaming sites.

Keep in mind that there are other sites that absolutely will not allow you to connect with your VPN turned on. If you encounter such a site, you might want to try connecting to a different server from your VPN. There’s a high likelihood that one server from your VPN provider is blocked, while another server works just fine. There are no guarantees. Some sites simply will not allow a VPN connection, regardless of which server you are using. Expect your results to vary as widely as there are sites disallowing VPN connections. Essentially, it’s a crap-shoot as to whether you can circumvent their blocking of VPN connections.

Let’s say you live in Denver, CO, and you go on a business trip to Paris. While staying in your hotel, you decide that you want to watch your favorite Netflix show. However, that show is not available in Europe on Netflix. Using your VPN, you can connect to a VPN server in the U.S., enabling you to watch your Netflix show from your Paris hotel room.

It’s also good to consider the connection speeds of the VPN you’re using. All of the top-tier VPN providers can accommodate the bandwidth demands that streaming services place on them. Other VPN providers, especially the “free” VPN providers, often don’t have the necessary bandwidth to stream content from streaming service providers.

Conclusion

Without a doubt, using a quality VPN provider will help safeguard your data and privacy. In today’s surveillance-fueled world that’s looking to amass as much of your personal and private information as possible, that’s definitely a good thing.

Be sure to do your own research to make sure that the VPN provider you choose will fulfill your needs. I’m not much of a user of streaming services (despite having access to a handful of them, and none of them are Netflix), but every user has different needs. Streaming is not one of my use cases, generally.

While I’m aware of the VPN services offered and built into many of the more popular browsers, those VPN services will ONLY protect you while using that particular browser. If you download torrents, use a messaging program/app, or do anything else online that doesn’t require a browser, those browser-specific VPNs WILL NOT protect any data not viewed inside that web browser. So, for me, they are of very limited benefit or use. While it may be perceived

as being better than nothing, it's not much better than "nothing."

As I've mentioned previously in other articles, I use my VPN to provide a greater sense of privacy and to safeguard my data. Like I've said before, when I send a snail mail letter, I have a reasonable expectation that the letter will remain private between me and the intended recipient. I don't think it's at all unreasonable to expect a similar level of privacy in my online activities.

My use of a VPN aids in that protection of my data and privacy.



Screenshot Showcase



Posted by tbs, on April 2, 2025, running KDE.

**Does your computer run slow?
Are you tired of all the "Blue Screens
of Death" computer crashes?**



**Are viruses,
adware, malware &
spyware slowing
you down?**

**Get your PC back
to good health
TODAY!**

Get



Download your copy today! FREE!

Typst Cookbook, Part 1

by David Pardue (kalwisti)

I have been [experimenting](#) off and on with Typst for six months, using it increasingly for my personal projects: letters, notes, and converting my old thesis. While learning new software, I find it more productive to adopt a hands-on, practical approach. I start writing something; when I get stuck, I turn to Typst's thorough [documentation](#), their new [forum](#), the Typst [subreddit](#), or a general DuckDuckGo search. This technique almost always leads to a solution.

I was inspired by a Spanish-language [manual](#), *Typst: Primeros pasos* ['Typst: First Steps'], written by ToniGL68. He chose a cookbook-type format with numerous examples rather than focusing on theory. I would like to share some of his “recipes” with you, as well as offer intermediate-level tips of my own. I hope these examples will help you use Typst more efficiently; they should work both within Typst's [web app](#) and with the Typst compiler [installed locally](#).

Document Language

Typst's text function has a parameter called [lang](#), with which you can set the language for the entire document or parts of the document. There is also a [region](#) parameter which uses these [ISO codes](#).

Although the default is English, if a portion of your document is in Spanish, you can type:

```
#set text(lang:"es", region:"eu")
```

to configure Typst for Spanish-language use with “European Union” as the region. (Adjust the region code as necessary, e.g., “es” [Spain], “mx” [Mexico].)

To revert to English, just type

```
#set text(lang:"eng")
```

above the next English-language section.

The [lang](#) parameter allows the correct hyphenation pattern to be used, as well as the appropriate [smart quotes](#), as shown below with the guillemets (also known as “comillas españolas” [Spanish quotation marks]):

«De tal palo, tal astilla.»

Switching to a Non-Roman Script

Typst supports Unicode out of the box. So if you need to use a non-Roman script in your document, you can copy and paste that script into your text (provided that the appropriate font is installed on your system, and it supports the script for that specific language).

This technique works well for inserting snippets of a non-Roman script into your document, as we see with the Sanskrit [shloka](#) below:

```
#set text(font:"Kalimati")
```

क्रोधाद्रवति सम्मोहः सम्मोहात्स्मृतिविभ्रमः | स्मृतिभ्रंशाद् बुद्धिनाशो बुद्धिनाशात्प्रणश्यति

```
#set text(font:"Liberation Serif")
```

Shloka from the Bhagavad Gita (Chapter 2, verse 63)

"Anger leads to clouding of judgment, which results in bewilderment of memory. When memory is bewildered, the intellect gets destroyed; and when the intellect is destroyed, one is ruined."

Produces this output:

क्रोधाद्रवति सम्मोहः सम्मोहात्स्मृतिविभ्रमः | स्मृतिभ्रंशाद् बुद्धिनाशो बुद्धिनाशात्प्रणश्यति

Shloka from the Bhagavad Gita (Chapter 2, verse 63)

"Anger leads to clouding of judgment, which results in bewilderment of memory. When memory is bewildered, the intellect gets destroyed; and when the intellect is destroyed, one is ruined."

Note: After inserting the Sanskrit snippet, remember to switch back to your Roman-alphabet font with the code

```
#set text(font:"Liberation Serif")
```


As a second example, here is the Ancient Greek "parent" of the Latin phrase *quod erat demonstrandum* (Q.E.D.), placed by early mathematicians at the end of mathematical proofs.

```
#set text(font: "Gentium Plus")
ὅπερ ἔδει δεῖξαι (OEA)

#set text(font: "Liberation Serif")
Quod erat demonstrandum (Q.E.D.): 'what was required to be proved'
```

Generates the output below:

ὅπερ ἔδει δεῖξαι (OEA)

Quod erat demonstrandum (Q.E.D.): 'what was required to be proved'

If you work with any of the CJK (Chinese, Japanese, Korean) languages, you will be pleased to know that the recent release of Typst ver. 0.13 has taken steps to [improve CJK support](#). The new feature allows CJK Typst users to more easily write text that mixes their native language and English. (This situation is challenging because Roman-alphabet text and Chinese text are almost always typeset with different fonts.)

Interword / Interlinear Spacing

You can directly insert interword spacing using the **h** (horizontal spacing) function, and interlinear spacing with the **v** (vertical spacing) command:

```
Horizontal #h(1cm) spacing.
#v(1cm)
And some vertical too!
```

The result is shown below:

Horizontal spacing.

And some vertical too!

Full-width Horizontal Rule

To create a solid line (with a thickness of two points) that spans the width of your document, type:

```
#line(length: 100%, stroke: 2pt)
```

Tables

If you need to incorporate tables into your writing, Typst is quite capable. The default table formatting is plain-Jane, but Typst's developers have been adding new features which allow users to style tables attractively.

As there are many options for creating and formatting tables, I recommend that you consult the documentation. A good starting point is Typst's ["Table Guide"](#). If you would prefer a video tutorial, the best one that I found was produced by Isaac Weintraub for his [BamDone](#) YouTube channel. He walks through the process of creating tables and demonstrates various methods of changing their format (from minute 13:01 until 34:50).

The basic table below was produced with this input:

```
#table(
  columns: 3,
  [*Product*], [*Quantity*], [*Price*],
  [Rice], [1002], [3,50€],
  [Artichokes (canned)], [207], [2,96€],
  [Dishwasher detergent], table.cell(colspan: 2)[Out of stock],
)
```

Product	Quantity	Price
Rice	1002	3,50€
Artichokes (canned)	207	2,96€
Dishwasher detergent	Out of stock	

*Note: The merged cell in the bottom right corner was achieved with the **table.cell** function's **colspan** argument. The "2" specifies that you want your cell to span two columns.*

Here is a table with the same data but formatted with a more "businesslike" appearance:

```
#table(
  stroke: none,
  columns: (3),
  [*Product*],          table.vline(),          [*Quantity*],
  table.vline(start:0, end:3, stroke:1pt), [*Price*],
  table.hline(),
  [Rice], [1002], [3,50€],
  [Artichokes (canned)], [207], [2,96€],
  [Dishwasher detergent],          table.cell(align:
center,colspan: 2,fill: red.transparentize(70%)) [Out
of stock],
)
```

Product	Quantity	Price
Rice	1002	3,50€
Artichokes (canned)	207	2,96€
Dishwasher detergent	Out of stock	

Note: "stroke: none" turns off the default strokes that differentiate between rows and columns. The `table.hline` element produces the horizontal line under the first row. The `table.vline` element produces the vertical lines after the first and second columns. With the second vertical line, the "start:0" and "end:3" arguments specify that the line begins before the first row (i.e., at the top of the table) and ends after the third row.

The arguments in the `table.cell` function specify this cell should span two columns, be centered and filled with red color. The `transparentize` argument makes a color more transparent by a given factor (70% in this example).

Captioning and Referencing Tables

In his video, Isaac Weintraub suggests using the `figure` function to make a clear connection between your table(s) and your document text. Wrapping a table in the figure function allows you to caption and reference your table, thereby saving you future work if you need to shift the table to a

different location/section of your document. It also lets you use the figure's placement parameter to float it to the top or bottom of a page.

The code block below creates a fairly complex table listing current PCLinuxOS mirrors:

```
#figure(
  caption: [PCLinuxOS Mirrors],
  table(
    stroke: 0.1pt,
    columns: (6),
    table.cell(fill: gray.transparentize(80%))
    [*Continent*], table.cell(fill:
gray.transparentize(80%)) [*Flag*], table.cell(fill:
gray.transparentize(80%)) [*Country*], table.cell(fill:
gray.transparentize(80%)) [*City*], table.cell(fill:
gray.transparentize(80%)) [*Institution / Company*],
    table.cell(fill: gray.transparentize(80%)) [*URL
(Partial)*],
    table.hline(start:0, end:6, stroke:2pt),
    [Asia], table.vline(start:0, stroke:1pt),
    image("jp.png", width: 50%), [Japan], [Nomi], [JAIST
(Japan Advanced Inst. of Science and Technology)],
    [ftp.jaist.ac.jp],
    [Asia], image("sg.png", width: 50%), [Singapore],
    [Singapore], [Freedif Open Source Mirror],
    [mirror.freedif.org],
    [Australia], image("au.png", width: 50%), [Australia],
    [ ], [AARNet], [mirror.aarnet.\ edu.au],
    [Australia], image("au.png", width: 50%), [Australia],
    [Adelaide (?)], [Internode], [mirror.internode.\
on.net],
    [Europe], image("bg.png", width: 50%), [Bulgaria],
    [Ruse], ["Angel Kanchev" University of Ruse],
    [mirrors.uni-ruse.bg],
    [Europe], image("fr.png", width: 50%), [France],
    [Paris], [Institut Pierre-Simon Laplace], [distrib-
coffee.\ ipsl.jussieu.fr],
    [Europe], image("de.png", width: 50%), [Germany],
    [Erlangen-Nürnberg], [Friedrich-Alexander-
Universität], [ftp.fau.de],
    [Europe], image("gr.png", width: 50%), [Greece],
    [Rethymno], [University of Crete Computer Center],
    [ftp.cc.uoc.gr],
    [Europe], image("nl.png", width: 50%), [The
```



```
Netherlands], [Amsterdam], [We Are Triple],
[pclinuxos.mirror. \ wearetriple.com],
[Europe], image("nl.png", width: 50%), [The
Netherlands], [Ede (?)], [NLUUG (The Netherlands Local
Unix User Group)], [ftp.nluug.nl],
[North America], image("us.png", width: 50%), [USA],
[Princeton, New Jersey], [Princeton University],
[mirror.math.\ princeton.edu],
[South America], image("br.png", width: 50%),
[Brazil], [Curitiba], [Universidade Federal do
Paraná], [pclinuxos.c3sl.\ ufpr.br],
[(Worldwide)], image("united-nations.png", width:
50%), [ ], [ ], [ ], [mirrors.cicku.me],
)
)<pclos-mirrors>
```

PCLOS Mirrors Table (as figure with images)

Continent	Flag	Country	City	Institution / Company	URL (Partial)
Asia		Japan	Nomi	JAIST (Japan Advanced Inst. of Science and Technology)	ftp.jaist.ac.jp
Asia		Singapore	Singapore	Freedif Open Source Mirror	mirror.freedif.org
Australia		Australia		AARNet	mirror.aarnet.edu.au
Australia		Australia	Adelaide (?)	Internode	mirror.internode.on.net
Europe		Bulgaria	Ruse	"Angel Kanchev" University of Ruse	mirrors.uni-ruse.bg
Europe		France	Paris	Institut Pierre-Simon Laplace	distrib-coffee.ipsl.jussieu.fr
Europe		Germany	Erlangen-Nürnberg	Friedrich-Alexander-Universität	ftp.fau.de
Europe		Greece	Rethymno	University of Crete Computer Center	ftp.cc.uoc.gr
Europe		The Netherlands	Amsterdam	We Are Triple	pclinuxos.mirror.wearetriple.com
Europe		The Netherlands	Ede (?)	NLUUG (The Netherlands Local Unix User Group)	ftp.nluug.nl
North America		USA	Princeton, New Jersey	Princeton University	mirror.math.princeton.edu
South America		Brazil	Curitiba	Universidade Federal do Paraná	pclinuxos.c3sl.ufpr.br
(Worldwide)					mirrors.cicku.me

Note: The "caption: [PCLinuxOS Mirrors]" will add the caption as a named argument below the table. I filled the top row's cells with a partially transparent gray color. The flag icons were imported/stored in my project folder in VSCode. The table.vline element produces a vertical line after the first column.

I gave this table a label—in angle brackets (<pclos-mirrors>). The label tells Typst to remember this element and make it referenceable under this name throughout your document. You can then refer to it in your text by typing: " @pclos-mirrors ". Typst will print a nicely formatted reference, and automatically update the label if the table's number changes.

Thus typing

Currently available PCLinuxOS mirrors are shown in @pclos-mirrors.

produces:

Table 1: PCLinuxOS Mirrors				

Currently available PCLinuxOS mirrors are shown in Table 1.

In the output, "Table 1" is a hyperlink; clicking on it will take you directly to that table.

Inserting Table from CSV File

Typst has a cool function called `csv` which creates a table by reading structured data from a .csv file. The simple table below was automatically generated by Typst when I imported the file baseball-catchers-list.csv into my project folder, using this syntax:

```
#table(
//stroke: none,
columns: 5,
..csv("baseball-catchers-list.csv").flatten(),
)
```

(Note: The " // " comments out the second line of that code block. This means the table will have the default stroke lines, black with 1pt thickness.)

Name	Team	Position	Height (in.)	Weight (lb.)
Adam Donachie	BAL	Catcher	74	180
A.J. Pierzynski	CWS	Catcher	75	245
Doug Mirabelli	BOS	Catcher	73	220
Victor Martinez	CLE	Catcher	74	190
Mike Piazza	OAK	Catcher	75	215
Jorge Posada	NYN	Catcher	74	205
Ivan Rodriguez	DET	Catcher	69	218
Rene Rivera	SEA	Catcher	70	190
Josh Paul	TB	Catcher	73	200
Jason LaRue	KC	Catcher	71	200
Gerald Laird	TEX	Catcher	74	220

Two Images Side by Side Using #figure() and #grid()

The next example will illustrate how to place two images side by side, using the **grid** function—and wrapping it in the figure function.

Although the grid function is somewhat similar to the table function, they are intended for different uses. While the table element is intended for presenting data, the grid element is intended for presentation and layout purposes (i.e., dividing the workspace into cells/blocks). Within each grid's cell, you may add elements such as text, lists, tables, images, etc. Each cell may be formatted independently, if you wish.

The two MLB teams below have a historically intense rivalry:

```
#figure(
caption: [A traditional MLB rivalry],
grid(
columns: (45%,1fr,45%),
row-gutter: 0.5em,
[#image("ny-yankees-logo.png",height:2cm)],
[],
[#image("bos-red-sox-logo.png",height:2cm)],
[New York Yankees], [], [Boston Red Sox]
)
)
```

<fig-baseball-logos>

The source code above produces this output:

The two MLB teams below have a historically intense rivalry:



Figure 3: A traditional MLB rivalry

Note: A grid's sizing is determined by what the Typst developers call "track size" (which is specified in the argument). In this example, the argument

columns: (45%,1fr,45%)

specifies that Column 1 (Yankees logo) and Column 3 (Red Sox logo) are each 45% of the total length. The "1fr" is a "fractional length" which means that once all the other tracks have been sized, the remaining space will be divided among the fractional tracks according to their fractions.

The layout shown in the screenshot above has three columns and two rows. There is a gutter of 0.5em

row-gutter: 0.5em

separating the two rows. The caption was created with

caption: [A traditional MLB rivalry]

One handy trick that can help us visualize the grid layout is to use Typst's **rect** (rectangle) function. This—together with a gray fill—will emphasize the area of cells we are working with. Using that technique with our current example, we will see the following layout:

Yankees logo (image)	[1fr]	Red Sox logo (image)
TeamName: New York Yankees (text)	[1fr]	TeamName: Boston Red Sox (text)

Figure 1: A traditional MLB rivalry

The code snippet to generate that output is:

```
// We use `rect` to emphasize the
// area of cells.
#set rect(
  inset: 8pt,
  fill: rgb("e4e5ea"),
  width: 100%,
)

#figure(
  caption: [A traditional MLB rivalry],
  grid(
    columns: (45%, 1fr, 45%),
    row-gutter: 0.5em,
    rect[Yankees logo (image)],
    [[1fr]],
    rect[Red Sox logo (image)],
    rect[TeamName: New York Yankees (text)], [[1fr]],
    rect[TeamName: Boston Red Sox (text)]
  )
)<fig-baseball-logos>
```

Thanks to Typst's fast, incremental compilation, it is easy to make on-the-fly adjustments to your table/grid settings and fiddle until you achieve a visually pleasing result. For instance, I experimented with changing the columns setting to

```
columns: (auto, auto, auto)
```


but I felt that the images were too closely spaced together:




New York YankeesBoston Red Sox
Figure 2: A traditional MLB rivalry

Boxes and Rectangles

Typst's **box** function allows you to create "boxes" within text; you can apply a specific format or even include content inside (such as a small image).

If you see this icon  you can be sure that "You Are Here".

If you see this icon  you can be sure that "You Are Here".

The **rect** (rectangle) function, like the box function, allows you to create a rectangle in which you may include elements, borders, fill, auto-sizing of content, etc. but it creates a separate "block" rather than being inserted into the current line:

#rect[This is a text box.] produces this output:

This is a text box.

You can fill the rectangle with a background color:

```
#rect(fill: luma(240))[Highlighted text ...#lorem(10)]
```

Highlighted text ...Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do.

You can apply borders, radii, dimensions, centering, as well as configuring color transparency with the "transparentize(%)" operation. The snippet below generates an understated callout box:

```
#align(center) [#rect(fill:
blue.transparentize(90%),stroke: 0.2pt, radius: 3pt,
width: 70%) [#align(left) [Sample text ...#lorem(30)]]]
```

Sample text ...Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri.



A Basic Letter

Although there are several letter templates available via Typst Universe, if you just need a simply formatted letter, you can create one quickly using Typst's out-of-the-box functionality. BamDone demonstrates how to compose a letter in thirty seconds.

```
#set page(
  paper: "us-letter",
  margin: (x:0.75in, y:1in)
)

#set text(
  font: "Liberation Serif",
)

#grid(
  columns: (lfr,auto),
  [],align(left)[
    Sender Name\
    Sender Address\
    City, State, ZIP code\
    Phone Number\
    #link("mailto:John.Doe@aol.com")
  ]
)
```

```
Recipient Name\
Recipient Address\
City, State, ZIP code\
```

```
Dear Recipient Name,
```

```
I am writing to request ...
```

```
I would also like to say these things ...
```

```
In closing, I will restate my main point ...
```

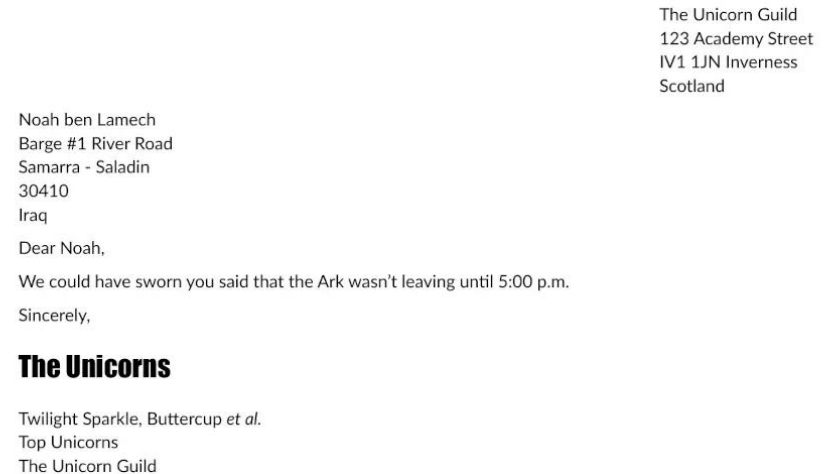
```
(This letter uses no external packages --- only what
Typst provides by default.)
```

```
Sincerely,\
```

```
#text(font: "Impact", size:18pt) [The Author]
```

```
First Name Last Name\
Impressive Title of Position\
Company / Institution
```

When you finish filling out this template with appropriate information, the letter's format will look something like the screenshot below:



```
Noah ben Lamech
Barge #1 River Road
Samarra - Saladin
30410
Iraq

Dear Noah,

We could have sworn you said that the Ark wasn't leaving until 5:00 p.m.

Sincerely,

The Unicorns

Twilight Sparkle, Buttercup et al.
Top Unicorns
The Unicorn Guild
```

Additional Resources

If you have a reading knowledge of Spanish, the manual by ToniGL68 is an excellent resource. His introduction to Typst adopts a cookbook-type format with numerous examples. The guide includes source-code "recipes" that you can work through while learning more about Typst.

[Introduction to Typst](#)

Typst: Primeros pasos. ["Typst: First Steps"]. ver. 2.0. 24 Jan. 2025.

If you are signed in to Typst's web app, you can access Toni's project with read-only privileges:

[Typst Web App](#)

Typst Documentation. "Table Guide."

Typst Documentation

BamDone [Isaac Weintraub]. "Getting Started with Typst - Some Tables (S01E06)." YouTube, 27 Jun. 2024. (35 min., 34 sec.)

Getting Started with Typst

"Composing a Letter with Typst in 30 Seconds." YouTube, 26 May 2024. (0 min., 28 sec.)

Composing a Letter in 30 secs.

I am planning to write a continuation of this cookbook for next month's magazine issue. In the meantime, I hope this will encourage you to further explore Typst's functionality.

If you are interested in seeing a Typst-generated replica of this article, I uploaded the PDF [11 p., 497 kB] to my [PCLOS Cloud](#) account and publicly shared it from there. The document's body typeface is Source Serif Pro, and the headings use Source Sans Pro.



linuxfordummies.org

There Are No Stupid Questions

Want To Help?

*Would you like to help
with the PCLinuxOS Magazine?
Opportunities abound. So get involved!
You can write articles, help edit articles,
serve as a "technical advisor" to insure
articles are correct, create artwork,
or help with the magazine's layout.
Join us on our Google Group mailing list.*



Like Us On Facebook!
The PCLinuxOS Magazine
PCLinuxOS Fan Club



Screenshot Showcase



Posted by Snubbi, on April 2, 2025, running Mate.

How Do You Solve A Problem Like Google Search? Courts Must Enable Competition While Protecting Privacy

by **Mitch Stoltz**

Electronic Frontier Foundation

Reprinted under Creative Commons [License](#)

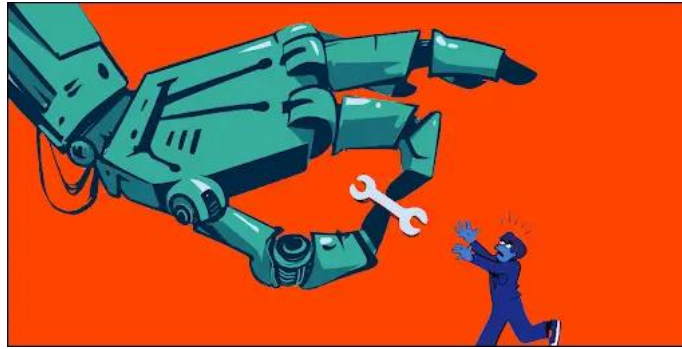
Can we get from a world where Google is synonymous with search to a world where other search engines have a real chance to compete? The U.S. and state governments' bipartisan [antitrust suit](#), challenging the many ways that Google has maintained its search monopoly, offers an opportunity.

Antitrust enforcers have [proposed](#) a set of complementary remedies, from giving users a choice of search engine, to forcing Google to spin off Chrome and possibly Android into separate companies. Overall, this is the right approach. Google's dominance in search is too entrenched to yield to a single fix. But there are real risks to users in the mix as well: Forced sharing of people's sensitive search queries with competitors could seriously undermine user privacy, as could a breakup without adequate safeguards.

Let's break it down.

The Antitrust Challenge to Google Search

The Google Search antitrust [suit](#) began in 2020 under the first Trump administration, brought by the Department of Justice and 11 states.



(Another 38 states filed a [companion suit](#).) The heart of the suit was Google's agreements with mobile phone makers, browser makers, and wireless carriers, requiring that Google Search be the default search engine, in return for revenue share payments including up to \$20 billion per year that Google paid to Apple. A [separate case](#), filed in 2023, challenged Google's dominance in online advertising. Following a bench trial in summer 2023, Judge Amit Mehta of the D.C. federal court found Google's search placement agreements to be illegal under the Sherman Antitrust Act, because they foreclosed competition in the markets for "general search" and "general search text advertising."

The antitrust enforcers proposed a set of remedies in fall 2024, and filed a revised version this month, signalling that the new administration remains committed to the case. A hearing on remedies is scheduled for April.



The Obvious Fix: Ban Search Engine Exclusivity and Other Anticompetitive Agreements

The first part of the government's remedy proposal bans Google from making the kinds of agreements that led to this lawsuit: agreements to make Google the default search engine on a variety of platforms, agreements to pre-install Google Search products on a platform, and other agreements that would give platforms an incentive not to develop a general search engine of their own. This would mean the end of Google's pay-for-placement agreements with Apple, Samsung, other hardware makers, and browser vendors like Mozilla.

In practice, a ban on search engine default agreements means presenting users with a screen that prompts them to choose a default search engine from among various competitors. Choice screens aren't a perfect solution, because people tend to stick with what they know. Still, [research shows](#) that choice screens can have a positive impact on competition if they are implemented thoughtfully. The court, and the technical committee appointed to oversee Google's compliance, should apply the lessons of this research.

It makes sense that the first step of a remedy for illegal conduct should be stopping that illegal conduct. But that's not enough on its own. Many users choose Google Search, and will continue

How Do You Solve A Problem Like Google Search? Courts Must Enable Competition While Protecting Privacy

to choose it, because it works well enough and is familiar. Also, as the evidence in this case demonstrated, the walls that Google has built around its search monopoly have kept potential rivals from gaining enough scale to deliver the best results for uncommon search queries. So we'll need more tools to fix the competition problem.

Safe Sharing: Syndication and Search Index

The enforcers' proposal also includes some measures that are meant to enable competitors to overcome the scale advantages that Google illegally obtained. One is requiring Google to let competitors use "syndicated" Google search results for 10 years, with no conditions or use restrictions other than "that Google may take reasonable steps to protect its brand, its reputation, and security." Google would also have to share the results of "synthetic queries"—search terms generated by competitors to test Google's results—and the "ranking signals" that underlie those queries. Many search engines, including DuckDuckGo, use syndicated search results from Microsoft's Bing, and a few, like Startpage, receive syndicated results from Google. But Google currently limits re-ranking and mixing of those results—techniques that could allow competitors to offer real alternatives. Syndication is a powerful mechanism for allowing rivals the benefits of scale and size, giving them a chance to achieve a similar scale.

Importantly, syndication doesn't reveal Google users' queries or other personal information, so it is a privacy-conscious tool.

Similarly, the proposal orders Google to make its index – the snapshot of the web that forms the basis for its search results - available to competitors. This too is reasonably privacy-conscious, because it presumably includes only data from web pages that were already visible to the public.

Scary Sharing: Users' "Click and Query" Data

Another data-sharing proposal is more complicated from a privacy perspective: requiring Google to provide qualified competitors with "user-side data," including users' search queries and data sets used to train Google's ranking algorithms. Those queries and data sets can include intensely personal details, including medical issues, political opinions and activities, and personal conflicts. Google is supposed to apply "security and privacy safeguards," but it's not clear how this will be accomplished. An order that requires Google to share even part of this data with competitors raises the risk of data breaches, improper law enforcement access, commercial data mining and aggregation, and other serious privacy harms.

Some in the search industry, including privacy-conscious companies like DuckDuckGo, argue that filtering this "click and query" data to

remove personally identifying information can adequately protect users' privacy while still helping Google's competitors generate more useful search results. For example, Google could share only queries that were used by some number of unique users. This is the approach Google already takes to sharing user data under the European Union's Digital Markets Act, though Google sets a high threshold that eliminates about 97% of the data. Other rules that could apply are excluding strings of numbers that could be Social Security or other identification numbers, and other patterns of data that may be sensitive information.

But click and query data sharing still sets up a direct conflict between competition and privacy. Google, naturally, wants to share as little data as possible, while competitors will want more. It's not clear to us that there's an optimal point that both protects users' privacy well and also meaningfully promotes competition. More research might reveal a better answer, but until then, this is a dangerous path, where pursuing the benefits of competition for users might become a race to the bottom for users' privacy.

The Sledgehammer: Splitting off Chrome and Maybe Android

The most dramatic part of the enforcers' proposal calls for an order to split off the Chrome browser as a separate company, and potentially also the Android operating system. This could be a powerful way to open up search competition. An independent Chrome and

How Do You Solve A Problem Like Google Search? Courts Must Enable Competition While Protecting Privacy

Android could provide many opportunities for users to choose alternative search engines, and potentially to integrate with AI-based information location tools and other new search competitors. A breakup would complement the ban on agreements for search engine exclusivity by applying the same ban to Chrome and Android as to iOS and other platforms.

The complication here is that a newly independent Chrome or Android might have an incentive to exploit users' privacy in other ways. Given a period of exclusivity in which Google could not offer a competing browser or mobile operating system, Chrome and Android could adopt a business model of monetizing users' personal data to an even greater extent than Google. To prevent this, a divestiture (breakup) order would also have to include privacy safeguards, to keep the millions of Chrome and Android users from facing an even worse privacy landscape than they do now.

The DOJ and states are pursuing a strong, comprehensive remedy for Google's monopoly abuses in search, and we hope they will see that effort through to a remedies hearing and the inevitable appeals. We're also happy to see that the antitrust enforcers are seeking to preserve users' privacy. To achieve that goal, and keep internet users' consumer welfare squarely in sight, they should proceed with caution on any user data sharing, and on breakups.



PCLinuxOS Magazine Graphics Special Edition, Volumes 1 - 4

Uhleash your GIMP & Inkscape skills. Over 160 tutorials. Grab your FREE copy now!

Screenshot Showcase



Posted by parnote, on April 22, 2025, running Xfce.

DOS GAMES ARCHIVE
WWW.DOSGAMESARCHIVE.COM

Set Up Your VPN's Servers Easily In NetworkManager

by Paul Arnote (parnote)

Why A VPN?

The number of people using Virtual Private Networks (VPNs) for their online activities is definitely on the upswing. Growing fears borne from the increased governmental oversight and overreach, along with the constantly increasing threat from the unfettered collection of personally identifiable private data by both governments and corporations, have made the use of a VPN an attractive option. VPNs are a very attractive option for those who value their privacy, and those who want to perform their online activities with a good bit more anonymity.

Of course, once you log into a site, everything you do is recorded by that site, so a VPN won't protect you from data collection about your activities on that site. It also (most likely) won't protect you from the "Facebook Pixel." That monstrosity is on a vast majority of websites (but NOT on the magazine website!), collecting information from all visitors, regardless if they are Facebook users or not. But a VPN will help protect you from having your activities recorded as you bounce from website to website.

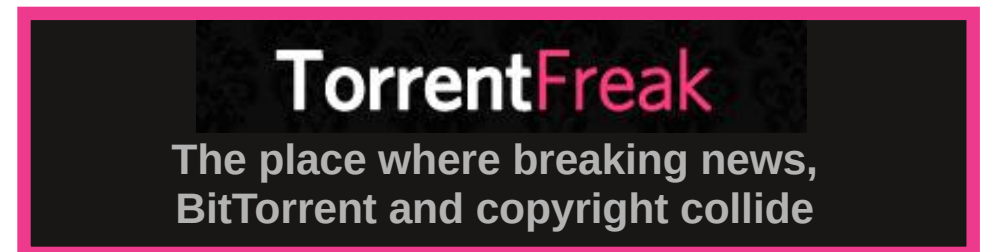
One of the entities tracking you is your ISP. Your ISP tracks your usage of your internet account to ensure you're not doing anything "illegal" (I put that in quotes because what's considered illegal can vary by your location), and to serve up targeted ads based on what they perceive your interests are. Of course, those "interests" are based on what sites you visit and what you do while you're there. Yes, it's called "metadata," and one or two pieces by themselves don't really reveal much about you. But, in aggregate with a huge number of pieces of metadata, it is quite revealing about what your interests are, who you are, your age, your income, whether you're married or single, if you have kids, what you like to eat, what your hobbies are, and a whole host of other data that really is no one else's business. Think of metadata as the pieces to a 10,000-piece jigsaw puzzle. One or two pieces

by themselves don't reveal much. But, a literal ton of pieces of metadata all put together (like that jigsaw puzzle) reveals far more about you than you can possibly imagine or realize.

Fortunately, by using a VPN, the connection between your computer and your VPN provider's server(s) is encrypted, so your ISP cannot see what you're doing. All they see is traffic. Just be certain that you don't have a DNS leak that's surreptitiously leaking your activities to your ISP. You can check for DNS leaks by heading over to one of two sites. The first site is [IPLeak.net](https://ipleak.net). There, it will display the IP address of the server you're connected to, and the IP address of the DNS server you're connected to. The second site is [DNSLeakTest.com](https://dnsleaktest.com). That second site checks ONLY the IP address of the DNS server that you are connected to.

On either site, if you see the IP address of your ISP displayed under the DNS section of the page, you're leaking data via your DNS server settings. A DNS leak will provide all the information your ISP needs to track your travels across the web, even if you use a VPN. Fortunately, that's easy enough to change. When setting up NetworkManager, you can specify an alternate DNS service provider. I use CloudFlare's free DNS servers (1.1.1.1 and 1.0.0.1), rather than Google's (8.8.8.8 and 8.8.4.4). Google already knows too much about me, so I don't need to "spoon-feed" my DNS information to them, as well.

Like I mentioned last month in my Firefox TOU article, I'm not really all that "conspiracy minded." However, I do expect some modicum of privacy in my online travels. I don't figure it's anyone else's concern what I'm



doing, where I'm going, to whom I'm talking, or anything else. It's kind of like a snail-mail letter. When I send a letter via snail-mail to another person, I have a reasonable expectation that the contents of that letter remain private between me and its intended recipient. My online activities should be no different.

I also am not of the mind, "I've done nothing wrong, so I have nothing to hide." It simply isn't anyone else's business what I do online. It's called privacy. How privacy online is treated so differently than that snail-mail letter is eternally baffling to me. The former is just a more modern version of the latter, yet the latter has far greater protections. Things that make your mind go "POOF!"

Also keep in mind that some sites don't like you connecting to them over a VPN. They are hellbent on preventing your use of a VPN on their site for a variety of reasons. In that case, you have three options. First, you can avoid that site altogether, which may not always be practical or possible. Second, you can try a different VPN server. One server may be "blocked," while another of the VPN servers from your VPN provider will work. Your third choice is to temporarily turn off your VPN while connecting to that site, and then resume/restart your VPN connection once you've completed your tasks on that particular site.

VPN's & NetworkManager

Until NetworkManager showed up for PCLinuxOS users, the choices for managing your online connection were either `net_applet` or `wicd`. And, when it came to setting up a VPN, I think there were only two people on the entire planet who could successfully set up a VPN connection using the tool in PCC. Seriously! I wasn't one of them, by the way. So, I came up with an alternate way to access my VPN under `net_applet`. Thankfully, with the arrival of NetworkManager, that "old" script is no longer needed, nor relevant any longer.

NetworkManager not only made it far, far easier to set up your online connection, but it also made setting up your VPN way, way, way easier. And, that's really what this article is all about.

Set Up Your VPN's Servers Easily In NetworkManager

Back in September 2023, something went awry with an update to NetworkManager. For some reason that I've since forgotten, users couldn't edit their connections in NetworkManager. The dialog where the NetworkManager connections were edited was crashing. Fortunately, that situation didn't last too long, as a subsequent update "righted the ship," so to speak. But, in discussing the [issue](#) in the forum, greater minds than mine came up with a solution for importing ALL of the servers for your VPN.

To be perfectly honest, I was planning on writing this script up for the magazine way back then, but I forgot about it ... until I messed up the install on my "travel" laptop (which I talked about in the March 2025 issue), and went to reinstall everything after replacing the SSD in that laptop. Of course, I wanted access to my VPN from my travel laptop, so that meant revisiting the script(s) that came out of that forum discussion.

And, until this script came along to import all of the available VPN servers for your given VPN (my VPN provider is Private Internet Access, a.k.a. PIA), I had only ever had no more than six of the 99+ available PIA servers across the world set up for my own use. I had set each up manually ... by hand. But, the script made all 99 VPN servers accessible to me for the first time!

Before you can proceed, however, you will need to download the OpenVPN files from your VPN provider. I tend to use OpenVPN files that are labeled as having "strong" encryption. Hey, I don't want to make it easy for anyone to be able to spy on my online activities. Just unpack the archive file containing your OpenVPN files into a directory of your choosing. For the purposes of this script, you can unpack them into their own directory in your Downloads directory. However, to ensure that any user on my computer has access to the VPN (even though I am the only "defined" user on any of my computers), I tend to copy those files to `/etc/openvpn`. You are free to unpack them there, as well, if you choose. But, for the purposes of running the script, having them unpacked into their own directory in your Downloads directory will work just fine.

Below is the script that sixte came up with in the forum. I've added the line numbers to improve readability. You don't need to type them in. However,

do ensure that you make the script (and any of the ones that follow) executable after you type it in and save it, and before you try to run it.

```
1. #!/bin/bash
2. USERNAME="xxxxxxxxxxxxxxxxxx"
3. PASS="yyyyyyyyyyyyyyyyyy"
4.
5. for f in *.ovpn
6. do
7.     name=`basename -s .ovpn $f`;
8.     nmcli connection import type openvpn file $f
9.     nmcli connection modify "${name}" +vpn.data connection-type=password-tls
10.    nmcli connection modify "${name}" +vpn.data username="${USERNAME}"
11.    nmcli connection modify "${name}" +vpn.data password-flags="0"
12.    nmcli connection modify "${name}" +vpn.secrets password="${PASS}"
13. done
```

Open a terminal session, and change directories until you're in the directory where you've stored your OpenVPN files. You will need to replace the "xxxxxxxxxxxxxxxxxx" with the username for your VPN, and "yyyyyyyyyyyyyyyyyy" with the password for your VPN account.

In less than one minute, every OpenVPN server for your VPN will be imported and set up for your use in NetworkManager. On my computers, I call this script **vpn-import.sh**.

So, yes, in this version of the script, your username and password are "hard coded" into the script. If you're the only user on your computer, that might not be all that much of a security concern.

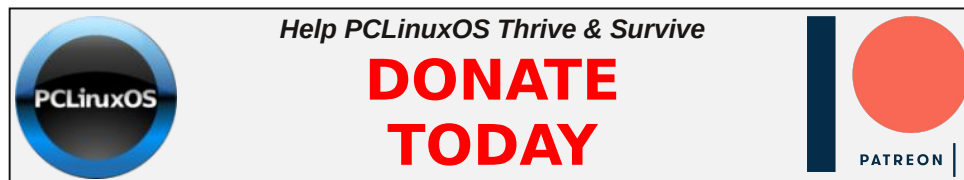
So, tbs came up with another version of the script (top of next column).

Set Up Your VPN's Servers Easily In NetworkManager

```
1. #!/bin/bash
2. #
3. read -p "User name: " vname
4. read -p "Password : " vpass
5. vpndir=<path-to-.ovpn-files>
6. cd $vpndir
7.
8. for vpnfile in *.ovpn; do
9.     nmcli connection import type openvpn file $vpnfile
10.    vpnnname=$(basename -s .ovpn $vpnfile)
11.    nmcli connection modify "${vpnnname}" +vpn.data connection-type=password-tls
12.    nmcli connection modify "${vpnnname}" +vpn.data password-flags="0"
13.    nmcli connection modify "${vpnnname}" +vpn.data username="${vname}"
14.    nmcli connection modify "${vpnnname}" +vpn.secrets password="${vpass}"
15. done
```

In his version of the script, the user is prompted to input the username and password. It's probably the most secure way to provide the username and password. There is no written "record" of those vital credentials. Everything is in the user's mind. Granted, you only have to enter this information once, when you initially import the OpenVPN files into NetworkManager. But for me, my VPN account's username is very difficult for me to remember. It's a cryptic ensemble of letters and numbers that I don't use often enough to memorize.

So, I remembered something that I used with my old-no-longer-relevant VPN script that I used to connect to my VPN with net_applet. With that, I stored all of my credentials in a simple text file, called login. I kept that file in /etc/openvpn, in the directory with the rest of the OpenVPN files on my computer. The format for those credentials couldn't possibly be more simple. On the first line is your username. On the second line is your password. That's it. Two lines. So, literally, the entire file looks something like this (top left of the next page):



your_username
your_password

Now, I can't put this "login" file in /etc/openvpn, due to permission issues. I want and need to run the script as a regular user, and a regular user can't access the files that belong to the root user. So, I did the next best thing, and stored the file elsewhere in my user's /home directory. To further "hide" it from prying eyes, I made it a hidden file, by making the first character a period. So, my most recent version of this script points to this hidden file, which I store in my /home directory. No subdirectory. Just in my /home directory. Since it's "hidden," no one really notices it. Of course, anyone looking at the script will know exactly where to find the file with my VPN login credentials, but they're going to have to work a little to access it. In other words, don't mistake obfuscation and hidden files for "security."

Here's my most recent version of that script:

```
1. #!/bin/bash
2.
3. # Your login information is stored in a plain text file
4. # with your username on the first line, and your
5. # password on the second line
6.
7. IFS=$'\n' read -d '' -r -a data < ~/.login
8. USERNAME="${data[0]}"
9. PASS="${data[1]}"
10.
11. for f in *.ovpn
12. do
13.     name=`basename -s .ovpn $f`;
14.     nmcli connection import type openvpn file $f
15.     nmcli connection modify "${name}" +vpn.data connection-type=password-tls
16.     nmcli connection modify "${name}" +vpn.data username="${USERNAME}"
17.     nmcli connection modify "${name}" +vpn.data password-flags="0"
18.     nmcli connection modify "${name}" +vpn.secrets password="${PASS}"
19. done
```

Set Up Your VPN's Servers Easily In NetworkManager

This version of the script reads my login credentials from that singular file in my /home directory, as shown in the first line that starts with IFS. That file is ~/.login. Notice the "period" before the name "login." That makes the file a hidden file. Now, you can call it whatever name you want and store it wherever you want (within your /home directory), as long as you point the read command to the appropriate file (you could call it "shopping-list" if you want). The read command fills an array with the lines from the .login file, and those lines are read into the string variables USERNAME and PASS, which are then used by the nmcli command.

Really, the ONLY difference between the three scripts is with the login credentials. In sixte's script, they are hard coded into the script. In tbs' script, it asks for the user to type them in, one at a time. In mine, the login credentials (username and password) are stored in a separate file, and read from that file. Everything else between the three scripts is exactly the same (from the for-do loop through to the end). If you're worried about security, then the first version is probably the least secure, the second version most secure, and the third version is somewhere in between. Of course, a user would have to be sitting at your computer for that information to be compromised (unless you accidentally share the script with your login information hard coded with someone else), and in that case, you probably have bigger things to worry about.

Caveats

If you're unfortunate enough to run this script twice (or more) on the same computer, you could end up with multiple entries among the VPN servers of your VPN provider.

Now, you could go in and manually delete all of those duplicate entries, and while that is doable, it'll take you some time. But, if you're interested in going down this path, NetworkManager saves its configuration files for the VPN servers at /etc/NetworkManager/system-connections.

Probably a quicker way is to just empty out that directory by deleting all of its contents, and just starting over with the import script.

Fortunately, tbs also came up with another script that makes this task much easier. He calls it **nm-vpn-delete**. Here it is:

```
1. #!/bin/bash
2.
3. # Shut down active VPN connection
4. vpnactive=$(nmcli con show --active | grep vpn | cut -d' ' -f1)
5. nmcli con down $vpncon
6.
7. # Delete existing VPN connections
8. vpnlist=$(nmcli con show | grep vpn | cut -d' ' -f1)
9. for vpncon in $vpnlist; do
10.     nmcli con down $vpncon
11.     nmcli con delete $vpncon
12. done
```

All you have to do is run this script to clear out the defined VPN connections, and then rerun the first script (whichever of the three versions you decide to use) to re-setup your VPN servers to choose from.

Summary

Without a doubt, the addition of NetworkManager to PCLinuxOS has made a HUGE improvement to managing network connections. And when it comes to setting up VPN connections, NetworkManager is light years ahead of the “old” method from PCC. Even setting them up manually is infinitely easier than that old method that virtually no one understood how to use. These scripts give you complete control over your VPN connections, and do so easily and very quickly.



The PCLinuxOS Magazine Special Editions!

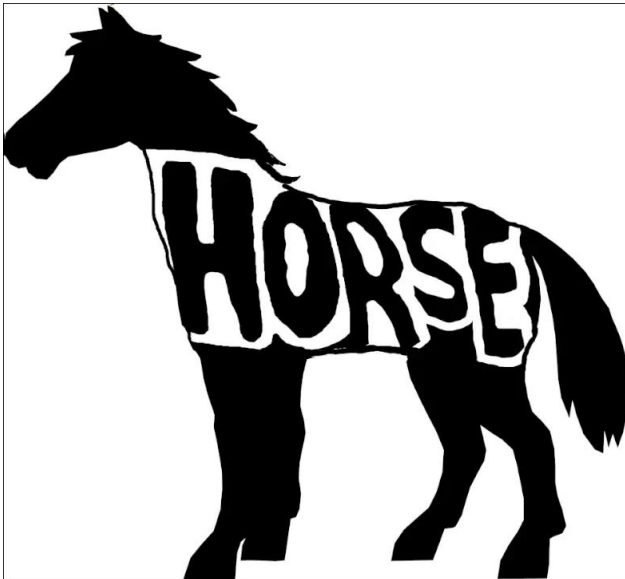


Get Your Free Copies Today!

GIMP Tutorial: Create A Word Art Logo

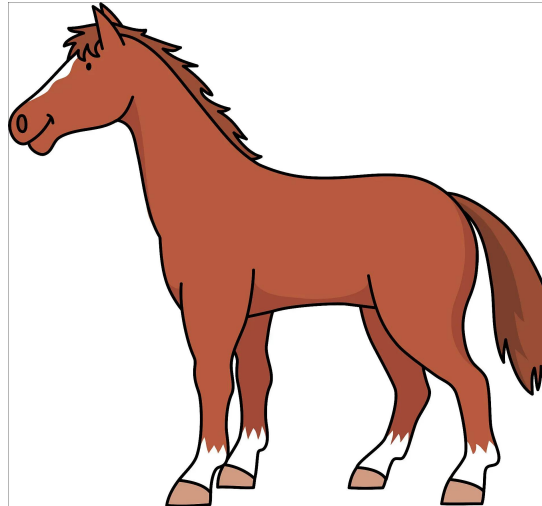
by Meemaw

I found a cool [video](#) the other day from [Logos by Nick](#), which described a method for creating a word art logo. It's very easy to do, but also requires multiple layers in GIMP. Nick states that most logos are usually made in a vector graphics program, such as Inkscape, but this particular project can be done really easily in GIMP.

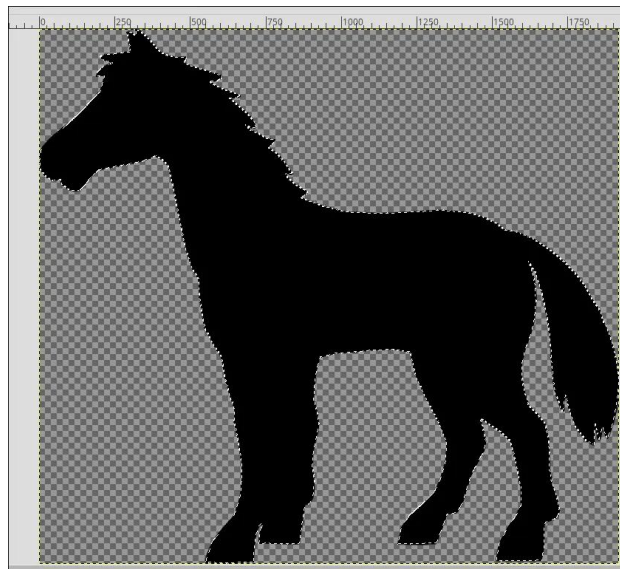


Let's do it. I chose a clipart image of a horse for my project, and loaded it into GIMP (center, top).

Add a new layer, filled with transparency. It will be on top of the clipart layer (where we want it).



Choose the **Paths** tool, and trace around the outside of the clipart. Close the path by clicking on the first node last. Choose the **Fill** tool, and fill your path with black.



Click on **Select > None** to get rid of your selection outline. You can also go into the layers and make your original clipart invisible.

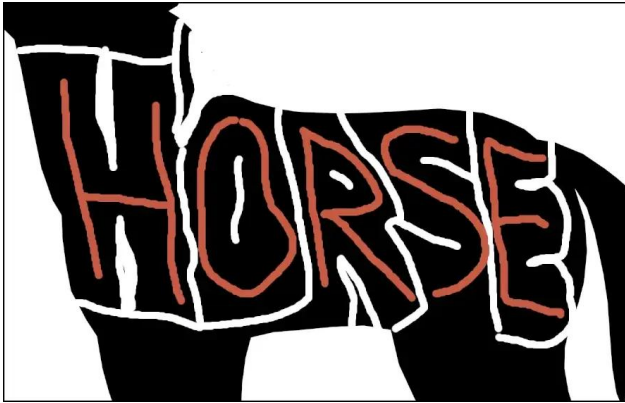
Add another transparent layer. To create the text, we'll use the **Paintbrush** tool about 10 or 15 px wide, with a different color (red, maybe). Write the word you want on the top layer. I used "HORSE".



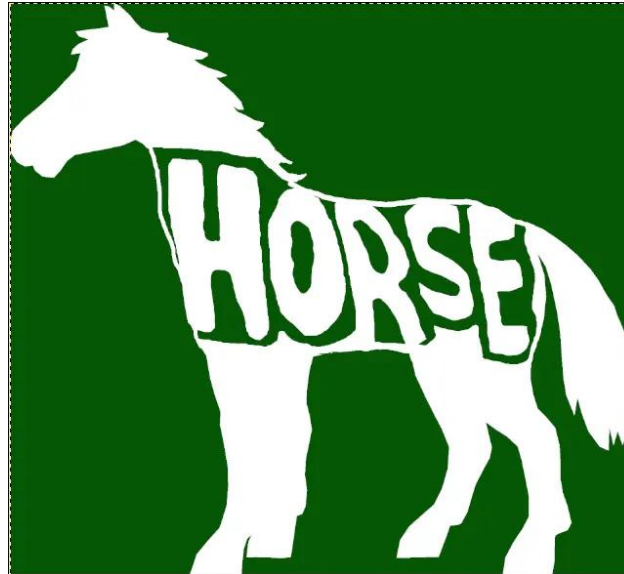
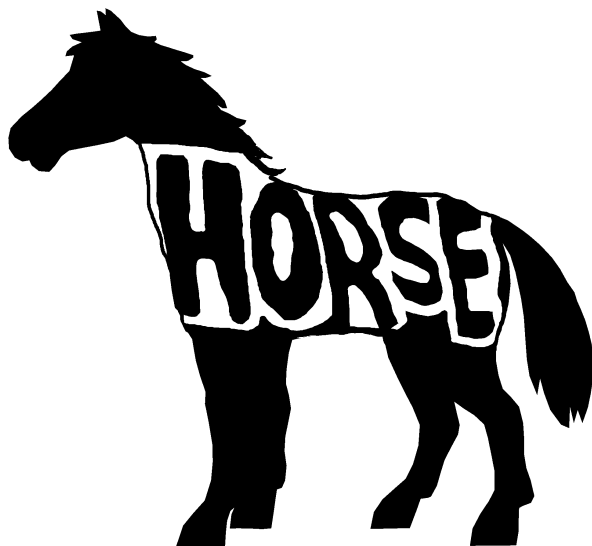
This is what we're going to use to make our word art.

Add another layer, filled with white, and move it below the filled path so you can see what you're doing. Set the opacity of the "letter" layer down a bit if you want. Select the filled layer. Change your tool to the eraser, about 10 or 15 px wide.

Now we're going to erase the black around and in between the letters, in preparation for the word art.



You can make your letters layer invisible now, if you want, and continue to erase the black until the letters look the way you want. If you erase too much, simply go back to the paintbrush tool, and paint some black back in. Alternate erasing and painting (if needed) until the letters look the way you want them. You can export it with the white layer visible, or you can make that layer invisible, and export it as a png, which will have transparency, so you can drop it on whatever background you want.



In the video, Nick also states that this can be taken into Inkscape and cleaned up further, if you wish to do it.

GIMP 3.0 is out, but I'm going to wait a bit to review the new features. It is available in an appimage, which I am not willing to use. Feel free to install the appimage, if you wish, and play with it yourself.



PCLinuxOS

Users Don't
Text
Phone
Web Surf
Facebook
Tweet
Instagram
Video
Take Pictures
Email
Chat
While Driving.

Put Down Your
Phone & Arrive
Alive.

Privacy On The Map: How States Are Fighting Location Surveillance

by [Rindala Alajaji](#)

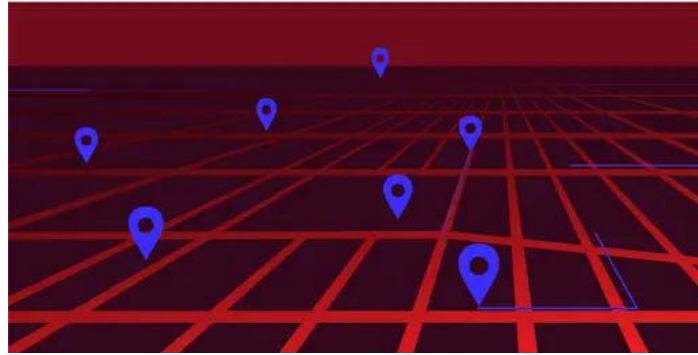
[Electronic Frontier Foundation](#)

Reprinted under Creative Commons [License](#)

Your location data isn't just a pin on a map—it's a powerful tool that reveals far more than most people realize. It can expose where you work, where you pray, who you spend time with, and, sometimes dangerously, where you seek healthcare. In today's world, your most private movements are harvested, aggregated, and sold to anyone with a credit card. For those seeking reproductive or gender-affirming care, or visiting a protest or an immigration law clinic, this data is a ticking time bomb.

Last year, [we sounded the alarm](#), urging lawmakers to protect individuals from the growing threats of location tracking tools—tools that are increasingly being used to target and criminalize people seeking essential reproductive healthcare.

The good news? Lawmakers in [California](#), [Massachusetts](#), [Illinois](#) and elsewhere are stepping up, leading the way to protect privacy and ensure that healthcare access and other exercise of our rights remain safe from invasive surveillance.



The Dangers of Location Data

Imagine this: you leave your home in Alabama, drop your kids off at daycare, and then drive across state lines to visit an abortion clinic in Florida. You spend two hours there before driving back home. Along the way, you used your phone's GPS app to navigate or a free radio app to listen to the news. Unbeknownst to you, this “free” app tracked your entire route and sold it to a data broker. That broker then mapped your journey and made it available to anyone who would pay for it. This is exactly what happened when privacy advocates used a tool called [Locate X](#), developed by Babel Street, to track a person's device as they traveled from Alabama — where abortion is completely banned — to Florida, where abortion access is severely restricted but still available.

Despite this tool being marketed as solely for law enforcement use, private investigators were able to access it by falsely claiming they would

work with law enforcement, revealing a major flaw in our data privacy system. In a time when government surveillance of [private personal decisions](#) is on the rise, the fact that law enforcement (and adversaries pretending to be law enforcement) can access these tools puts our personal privacy in serious danger.

The unregulated market for location data enables anyone, from law enforcement to anti-abortion groups, to access and misuse this sensitive information. For example, a data broker called [Near Intelligence](#) sold location data of people visiting Planned Parenthood clinics to an anti-abortion group. Likewise, law enforcement in Idaho used [cell phone location data](#) to charge a mother and her son with “aiding and abetting” abortion, a clear example of how this information can be weaponized to enforce abortion restrictions for patients and anyone else in their orbit.

States Taking Action

As we've seen time and time again, the collection and sale of location data can be weaponized to target many vulnerable groups—[immigrants](#), the [LGBTQ+ community](#), and anyone seeking [reproductive healthcare](#). In response to these growing threats, states like [California](#), [Massachusetts](#), and [Illinois](#) are leading the charge by introducing bills aimed at



regulating the collection and use of location data.

These bills are a powerful response to the growing threat. The bills are grounded in well-established principles of privacy law, including informed consent and data minimization, and they ensure that only essential data is collected, and that it's kept secure. Importantly, they give residents—whether they reside in the state or are traveling from other states—the confidence to exercise their rights (such as seeking health care) without fear of surveillance or retaliation.

This post outlines some of the key features of these location data privacy laws, to show authors and advocates of legislative proposals how best to protect their communities. Specifically, we recommend:

- Strong definitions,
- Clear rules,
- Affirmation that all location data is sensitive,
- Empowerment of consumers through a strong private right of action,
- Prohibition of “pay-for-privacy” schemes, and
- Transparency through clear privacy policies.

Strong Definitions

Effective location privacy legislation starts with clear definitions. Without them, courts may interpret key terms too narrowly—weakening the law's intent. And in the absence of clear judicial guidance, regulated entities may exploit ambiguity to sidestep compliance altogether.

The following are some good definitions from the recent bills:

- In the **Massachusetts** bill, “consent” must be “*freely given, specific, informed, unambiguous, [and] opt-in.*” Further, it must be free from dark patterns—ensuring people truly understand what they’re agreeing to.
- In the **Illinois** bill, a “covered entity” includes all manner of private actors, including individuals, corporations, and associations, exempting only individuals acting in noncommercial contexts.
- “Location information” must clearly refer to data derived from a device that reveals the past or present location of a person or device. The **Massachusetts** bill sets a common radius in defining protected location data: 1,850 feet (about one-third of a mile). The **California** bill goes much bigger: five miles. EFF has supported both radiuses.
- A “permissible purpose” (which is key to the minimization rule) should be narrowly defined to include only: (1) delivering a product or service that the data subject asked for, (2) fulfilling an order, (3) complying with federal or state law, or (4) responding to an imminent threat to life.

Clear Rules

“Data minimization” is the privacy principle that corporations and other private actors must not process a person’s data except as necessary to give them what they asked for, with narrow

exceptions. A virtue of this rule is that a person does not need to do anything in order to enjoy their statutory privacy rights; the burden is on the data processor to process less data. Together, these definitions and rules create a framework that ensures privacy is the default, not the exception.

One key data minimization rule, as in the **Massachusetts** bill, is: “*It shall be unlawful for a covered entity to collect or process an individual’s location data except for a permissible purpose.*” Read along with the definition above, this across-the-board rule means a covered entity can only collect or process someone’s location data to fulfil their request (with exceptions for emergencies and compliance with federal and state law).

Additional data minimization rules, as in the **Illinois** bill, back this up by restraining particular data practices:

- Covered entities can not collect more precise data than strictly necessary, or use location data to make inferences beyond what is needed to provide the service.
- Data must be deleted once it’s no longer necessary for the permissible purpose.
- No selling, renting, trading, or leasing location data – full stop.
- No disclosure of location data to government, except with a warrant, as required by state or federal law, on request of the data subject, or

an emergency threat of serious bodily injury or death (defined to not include abortion).

- No other disclosure of location data, except as required for a permissible purpose or when requested by the individual.

The **California** bill rests largely on data minimization rules like these. The **Illinois** and **Massachusetts** bills place an additional limit: no collection or processing of location data absent opt-in consent from the data subject. Critically, consent in these two bills is not an exception to the minimization rule, but rather an added requirement. EFF has supported both models of data privacy legislation: just a minimization requirement; and paired minimization and consent requirements.

All Location Data is Sensitive

To best safeguard against invasive location tracking, it's essential to place legal restrictions on the collection and use of all location data—not just data associated with sensitive places like reproductive health clinics. Narrow protections may offer partial help, but they fall short of full privacy.

Consider the example at the beginning of the blog: if someone travels from Alabama to Florida for abortion care, and the law only shields data at sensitive sites, law enforcement in Alabama could still trace their route from home up to near the clinic. Once the person enters a protected “healthcare” zone, their device would vanish from view temporarily, only to reappear shortly after they leave. This

gap in the tracking data could make it relatively easy to deduce where they were during that time, essentially revealing their clinic visit.

To avoid this kind of loophole, the most effective approach is to limit the collection and retention of all location data—no exceptions. This is the approach in all three of the bills highlighted in this post: **California**, **Illinois**, and **Massachusetts**.

Empowering Consumers Through a Strong PRA

To truly protect people's location privacy, legislation must include a strong [private right of action](#) (PRA)—giving individuals the power to sue companies that violate their rights. A private right of action ensures companies can't ignore the law and empowers people to seek justice directly when their sensitive data is misused. This is a top priority for EFF in any data privacy legislation.

The bills in **Illinois** and **Massachusetts** offer strong models. They make clear that any violation of the law is an injury and allow individuals to bring civil suits: “A violation of this [law] ... regarding an individual's location information constitutes an injury to that individual. ... Any individual alleging a violation of this [law] ... may bring a civil action ...” Further, these bills provide a baseline amount of damages (sometimes called “liquidated” or “statutory” damages), because an invasion of statutory privacy rights is a real injury, even if it is hard for the injured party to

prove out-of-pocket expenses from theft, bodily harm, or the like. Absent this kind of statutory language, some victims of privacy violations will lose their day in court.

These bills also override [mandatory arbitration clauses](#) that limit access to court. Corporations should not be able to avoid being sued by forcing their customers to sign lengthy contracts that [nobody reads](#).

Other remedies include actual damages, punitive damages, injunctive relief, and attorney's fees. These provisions give the law real teeth and ensure accountability can't be signed away in fine print.

No Pay-for-Privacy Schemes

Strong location data privacy laws must protect everyone equally—and that means rejecting “[pay-for-privacy](#)” schemes that allow companies to charge users for basic privacy protections. Privacy is a fundamental right, not a luxury add-on or subscription perk. Allowing companies to offer privacy only to those who can afford to pay creates a two-tiered system where low-income individuals are forced to trade away their sensitive location data in exchange for access to essential services. These schemes also incentivize everyone to abandon privacy.

Legislation should make clear that companies cannot condition privacy protections on payment, loyalty programs, or any other exchange of value. This ensures that everyone—regardless of income—has equal protection from

Privacy On The Map: How States Are Fighting Location Surveillance

surveillance and data exploitation. Privacy rights shouldn't come with a price tag.

We commend this language from the **Illinois** and **Massachusetts** bills:

A covered entity may not take adverse action against an individual because the individual exercised or refused to waive any of such individual's rights under [this law], unless location data is essential to the provision of the good, service, or service feature that the individual requests, and then only to the extent that this data is essential. This prohibition includes, but is not limited to: (1) refusing to provide a good or service to the individual; (2) charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties; or (3) providing a different level of quality of goods or services to the individual.

Transparency Through Clear Privacy Policies

It is helpful for data privacy laws to require covered entities to be transparent about their data practices. All three bills discussed in this post require covered entities to make available a privacy policy to the data subject—a solid baseline. This ensures that people aren't left in the dark about how their location data is being collected, used, or shared. Clear, accessible policies are a foundational element of informed consent and give individuals the information they need to protect themselves and assert their rights.

It is also helpful for privacy laws like these to require covered entities to prominently publish their privacy policies on their websites. This allows all members of the public – as well as privacy advocates and government enforcement agencies – to track whether data processors are living up to their promises.

Next Steps: More States Must Join

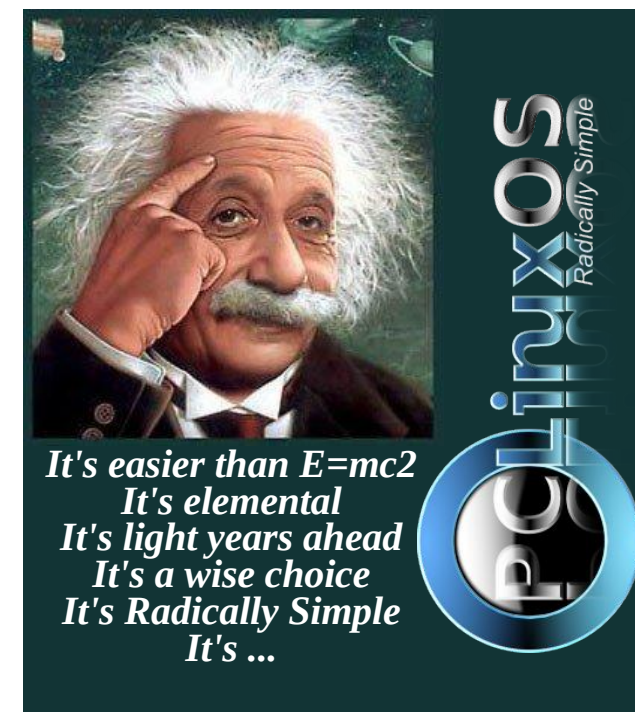
The bottom line is clear: location data is highly sensitive, and without proper protections, it can be used to harm those who are already vulnerable. The digital trail we leave behind can reveal far more than we think, and without laws in place to protect us, we are all at risk.

While some states are making progress, much more needs to be done. More states need to follow suit by introducing and passing legislation that protects location data privacy. We cannot allow location tracking to be used as a tool for harassment, surveillance, or criminalization.

To help protect your digital privacy while we wait for stronger privacy protection laws, we've published a guide specifically for how to minimize intrusion from [Locate X](#), and have additional tips on EFF's [Surveillance Self-Defense](#) site. Many general privacy practices also offer strong protection against location tracking.

If you live in **California**, **Illinois**, **Massachusetts** – or any state that has yet to

address location data privacy – now is the time to act. Contact your lawmakers and urge them to introduce or support bills that protect our sensitive data from exploitation. Demand stronger privacy protections for all, and call for more transparency and accountability from companies that collect and sell location data. Together, we can create a future where individuals are free to travel without the threat of surveillance and retaliation.





Download Your Free Copy Today

KDE
Mate
Xfce
LXQt



Openbox
Enlightenment
IceWM
Trinity

Does your computer run slow? Are you tired of all the "Blue Screens of Death" computer crashes?



Are viruses,
adware, malware
& spyware
slowing you down?
Get your PC
back to good health
TODAY!
Get



Download your copy today! FREE!



PCLOS-Talk
Instant Messaging Server



Sign up TODAY! <http://pclostalk.pclosusers.com>

Screenshot Showcase



Posted by mutse, on April 11, 2025, running Mate.

ICYMI: New Runway Safety Measures Coming To An Airport Near You

by Paul Arnote (parnote)

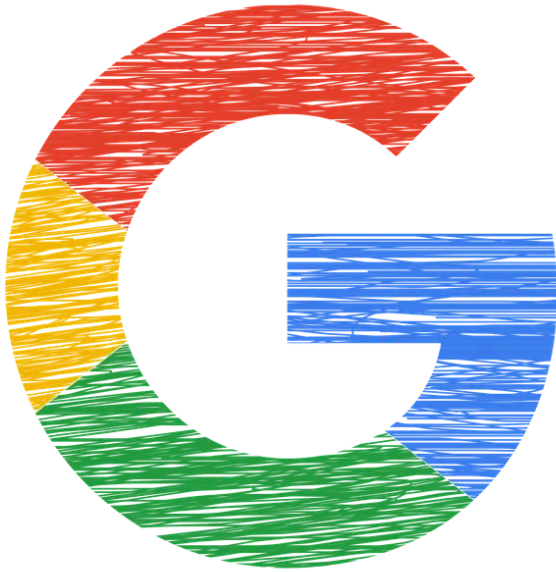


Image by [Elisa](#) from [Pixabay](#)

The European Commission has published preliminary findings on Alphabet and how it could be preventing competition, according to an [article](#) from TechRepublic. The concerns relate to two issues: self-preferencing in Google Search and “steering rules” in Google Play; these issues were looked into as part of a non-compliance investigation [opened](#) in March 2024. The DMA bans self-preferencing, which is when a dominant platform favours its own products or services over those of competitors. The Commission believes the way Alphabet presents Google Search results may steer customers

toward Google services, such as Shopping, Flights, or Hotels. Secondly, the Commission argues that the Play Store, Google’s mobile app marketplace, prevents app developers from directing consumers to alternative purchasing channels, such as their own website or third-party app stores. This limits their ability to offer better deals outside of Google’s platform. Google has made a series of changes in the last year to comply with the DMA, such as [temporarily](#) removing some Search Widgets and rejigging the layout of [Search results](#), but the Commission has determined that these steps are insufficient.

More than 300 organizations in critical infrastructure, including the medical, tech, and manufacturing sectors, have been victimized by a ransomware threat known as Medusa — and with [attacks](#) escalating significantly in the first few months of 2025, the FBI and the Cybersecurity and Infrastructure Agency (CISA) are advising companies to take steps now to secure their systems, according to an [article](#) from Lifehacker. Medusa is a ransomware-as-a-service (RaaS) software that, when deployed successfully, encrypts your data along with a threat to release stolen information unless you comply with ransom demands. According to the [CISA advisory](#), victims receive ransom notes requesting a response within 48 hours, or Medusa actors will reach out to them by phone or email. Victims are also listed on a data-leak

website alongside a countdown timer and ransom demands with direct links to cryptocurrency wallets. Victims can pay \$10,000 to add a day to the countdown—meanwhile, Medusa advertises the data for sale before the timer runs out. This “double extortion” approach forces payment to both decrypt locked files and prevent them from being released or sold (so even if you have a backup you can recover, you still face the threat of information being leaked). The Medusa ransomware was first identified in June 2021 and has since affected organizations across the medical, education, legal, insurance, technology, and manufacturing industries. According to the advisory, Medusa actors use common tricks like phishing campaigns and exploitation of unpatched software vulnerabilities to steal victims’ credentials and gain access to their systems. While much of the Medusa threat mitigation happens at the organizational level, there are a few things you as an individual can do to protect your accounts and—by extension—the company you work for.

A United States District Court for the Northern District of California judge has signed off on a settlement agreement between HP and its customers, who sued the company for issuing firmware updates that prevented their printers from working with non-HP ink and toner, according to an [article](#) from ArsTechnica. In December 2020, Mobile Emergency Housing Corp. and a company called Performance Automotive & Tire Center

filed a class-action complaint against HP [PDF], alleging that the company “wrongfully compels users of its printers to buy and use only HP ink and toner supplies by transmitting firmware updates without authorization to HP printers over the Internet that lock out its competitors’ ink and toner supply cartridges.” The complaint centered on a firmware update issued in November 2020; it sought a court ruling that HP’s actions broke the law, an injunction against the firmware updates, and monetary and punitive damages.



Image from Pixabay

The Federal Aviation Administration is deploying runway safety technology upgrades at 74 air traffic control towers in the U.S., the agency [announced](#) on March 19, 2025, and according to an [article](#) from AV Web. The Runway Incursion Device (RID) is designed to assist air traffic controllers by providing real-time alerts when a runway is occupied or closed. With the ability to monitor up to eight runways

simultaneously, the RID will replace various outdated systems currently in use at control towers, streamlining safety operations across the country. The RID is part of the FAA’s fast-tracked surface safety portfolio, which also includes the Surface Awareness Initiative (SAI) and the Approach Runway Verification (ARV) system. All are designed to improve overall safety on the ground.

The EU suspects that Apple has breached the Digital Markets Act due to the company not allowing third-party hardware to connect with its platforms, according to an [article](#) from TechRepublic. Fines for noncompliance with the DMA can be up to 10% of the company’s total worldwide turnover, rising to 20% in cases of repeated infringement. Apple has been slapped with two sets of guidance on how to comply with the Commission’s interoperability requirements, relating to iOS connectivity features and the process for handling interoperability requests from developers, respectively. A spokesperson for Apple told TechRepublic: “Today’s decisions wrap us in red tape, slowing down Apple’s ability to innovate for users in Europe and forcing us to give away our new features for free to companies who don’t have to play by the same rules. It’s bad for our products and for our European users.”

A new manufacturing plant in the northeastern Alberta community of Elk Point is blending hemp and other additives into concrete to make lightweight building blocks resistant to weather, fire and mold, according to an [article](#) from the CBC. The company, called [Asinikahtamwak](#) — in Cree it means “works

with rock” — operates from a 13,000-square-foot building on the south end of Elk Point, 215 kilometres northeast of Edmonton. The high-performance building blocks being made in Elk Point are the same size as traditional cinder blocks but weigh only half as much. Asinikahtamwak says other benefits include reduced noise transmission, better thermal insulation and reduced cracking.

ORACLE®

CLOUD

A sophisticated supply chain hack targeting Oracle Cloud has exfiltrated a staggering 6 million records, according to an [article](#) from eSecurityPlanet. CloudSEK’s XVigil uncovered that threat actor “rose87168” began selling the stolen data on March 21. The breach, exploiting a vulnerability in Oracle’s cloud infrastructure, now endangers over 140,000 tenants and has raised serious questions about cloud security practices. The breach appears to be linked to a well-known vulnerability — [CVE-2021-35587](#) — which affects Oracle Access Manager (OpenSSO Agent) in Oracle Fusion Middleware. According to FOIA data, the vulnerable endpoint, last updated on Sept. 27, 2014, allowed an unauthenticated attacker network access via HTTP. This easily exploitable flaw enabled a complete compromise of Oracle Access Manager, underscoring how outdated configurations and poor patch management can lead to large-scale security failures.

ICYMI: New Runway Safety Measures Coming To An Airport Near You

Microsoft is changing the look of the BSOD, according to an [article](#) from Lifehacker. The company announced the redesign in a Friday post on the Windows Insider [blog](#). (The Windows Insider program allows software testers to try out new Windows features early before Microsoft launches them to the public.) In addition to a number of other new features and changes testers can try, there's the new BSOD, which Microsoft says is “more streamlined” and “better aligns with Windows 11 design principles,” while maintaining the same technical information you'd expect from the traditional blue screen. During testing, the new BSOD is actually green, but will be black when it is rolled out to the public.

Tory Hunt, the owner of credential leak website HaveIBeenPwned, is notifying thousands of subscribers after falling for a MailChimp phishing scam — in which approximately 16,000 credentials were compromised, according to an [article](#) from TechRadar. In a [blog post](#), Hunt described the attack which led to the export of the credentials, in which he was emailed a fake ‘Sending

Privileged Restricted’ notification, which encouraged him to review his account through an email link. When Hunt followed the link, he was taken to a page and asked to enter his credentials, which, he notes, did not auto-complete from 1Password (a tell-tale sign). Moments later, ‘the penny dropped’, Hunt says, as he realized his mistake.



Image by [Fakhruddin Memon](#) from Pixabay

New Android malware is using Microsoft's .NET MAUI to fly under the radar in a new cybersecurity dust-up this week, according to an [article](#) from TechRepublic. Disguised as actual services such as banking and social media apps targeting Indian and Chinese-speaking users, the malware is designed to gain access to sensitive

information. Cybersecurity experts with McAfee's Mobile Research Team say that, while the threat is currently aimed at China and India, other cybercriminal groups could easily adopt the same method to target a broader audience.

An important focus of AI research is improving an AI system's factualness and trustworthiness. Even though significant progress has been made in these areas, some AI experts are pessimistic that these issues will be solved in the near future. **That is one of the main findings of a new report by The Association for the Advancement of Artificial Intelligence (AAAI), which includes insights from experts from various academic institutions (e.g., MIT, Harvard, and University of Oxford) and tech giants (e.g., Microsoft and IBM)**, according to an [article](#) from TechRepublic. The goal of the study was to define the current trends and the research challenges to make AI more capable and reliable so the technology can be safely used, wrote AAAI President Francesca Rossi. The report includes 17 topics related to AI research culled by a group of 24 “very diverse” and experienced AI researchers, along with 475 respondents from the AAAI community, she noted. Here are highlights from this AI research report.


If you're a gamer, beware a new malware that's pretending to be an ASUS utility, according to an [article](#) from Lifehacker. CoffeeLoader [impersonates](#) Armoury Crate, which manages ASUS and ROG software and peripherals, and infects your Windows machine with an infostealer that's nearly impossible to detect. According to an [analysis](#) by ZScaler,

FREE!

**Original SciFi Books
By PCLinuxOS's
Own arjaybe!**

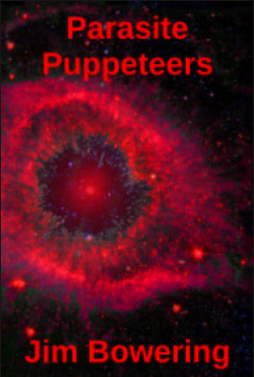
Download Today!

Green Comet




Jim Bowering

Parasite Puppeteers



Jim Bowering

The Francesians



Jim Bowering

once on your system, the CoffeeLoader malware delivers the [Rhadamanthys infostealer](#), which can extract credentials from applications like web browsers, email clients, crypto wallets, and even the password manager KeePass. CoffeeLoader then manages to evade most security tools on your device, including antivirus software and malware detectors, making it especially dangerous and difficult to catch. It does this in part by running on the graphics card (GPU), which security tools aren't as likely to scan, rather than your computer's CPU.



Image by [Gerd Altmann](#) from [Pixabay](#)

OpenAI has significantly [leveled up](#) the image generating capabilities of ChatGPT, as part of an update to the GPT-4o model [introduced](#) last May. **The new and improved AI image generator is out now for all ChatGPT users, although [free access](#) does have limits, with higher limits also in place for the \$20/month ChatGPT Plus plan,** according to an [article](#) from Lifehacker. Still, that's an improvement over the initial launch on March 25, as free image generation was [quickly pulled](#) after release due to heavy server loads. It's not clear right now what the limits for free and Plus users are, although CEO Sam Altman had previously [posted](#) that the goal is to allow free users three images per day.

All enterprise users of Gmail can now easily apply end-to-end encryption to their emails, according to an [article](#) from TechRepublic. Prior to April 1, 2025, this was a luxury reserved for big businesses with significant IT resources, but Google recognises that email attacks are on the rise across the board. Starting April 1, 2025, Gmail users can send end-to-end encrypted emails to others within their organisation; in the coming weeks, they will also be able to send encrypted emails to Gmail inboxes outside their organisation, with support for all email inboxes expected later this year. To get early access for E2EE emails in Gmail, fill out Google's Pre-General Availability Test [Application](#). Emails sent with Gmail's end-to-end encryption are extremely secure because only the sender has control over the encryption key, which is stored outside of Google's infrastructure. Users can click the padlock by the Bcc button and press Turn On under the Additional Encryption' option to apply it.

To celebrate 50 years of Microsoft, famous/infamous (depending on how you view him) co-founder of Microsoft **Bill Gates is "gifting" the source code for Altair Basic** to the world. You can view it [here](#). There's also a nice "write up" about his "philanthropic move" from the TechRepublic [here](#). The code is presented on Gates Notes complete with a backstory involving its creation. If nothing else, it makes for some interesting reading. Now, if only he'd release the source code for MS-DOS, Win31, WinXP and several other long-gone stalwarts of computing history ... well, that would be one helluva story! How monogamous is his gifting of the source code for a processor no longer

created, no longer in use, no longer available, and no longer a factor in serious computing? While it may be the "coolest code he's ever written," (his words, not mine) it fails to provide anything new in this current age of computers, other than a nostalgic peek at computing history and the events leading up to it. It did, however, give Microsoft its first "sale," and gave rise to the company we see today.



ESA

As part of ESA/Hubble's 35th anniversary celebrations, a new image series is being shared to revisit stunning Hubble targets that were previously released, according to the ESA Hubble Telescope [website](#). This image series combines new processing techniques with the latest data from Hubble to re-release these cosmic scenes for the public to enjoy. This new image showcases the dazzling young star cluster NGC 346. Although several images of NGC 346 have been released previously, this view

includes new data and is the first to combine Hubble observations made at infrared, optical, and ultraviolet wavelengths into an intricately detailed view of this vibrant star-forming factory. NGC 346 is located in the Small Magellanic Cloud, a satellite galaxy of the Milky Way that lies 200 000 light-years away in the constellation [Tucana](#). The Small Magellanic Cloud is less rich in elements heavier than helium — what astronomers call metals — than the Milky Way. This makes conditions in the galaxy similar to what existed in the early Universe. NGC 346 is home to more than 2500 newborn stars. The cluster's most massive stars, which are many times more massive than our Sun, blaze with an intense blue light in this image. The glowing pink nebula and snakelike dark clouds are the remnant of the birthsite of the stars in the cluster.

On Thursday, 27 March, the European Space Agency ([ESA](#)) sent its last messages to the [Gaia Spacecraft](#). **They told Gaia to shut down its communication systems and central computer and said goodbye to this amazing space telescope**, according to an [article](#) from The Conversation. Gaia was retired for a simple reason: after more than 11 years in space, [it ran out](#) of the cold gas propellant it needed to keep scanning the sky. The telescope did its last observation on 15 January 2025. The ESA team then performed testing for a few weeks, before telling Gaia to leave its home at a point in space [called L2](#) and start orbiting the Sun away from Earth. Its main mission was to produce a detailed, three-dimensional [map](#) of our galaxy, the Milky Way. To do this, it measured the precise positions and motions of [1.46 billion](#)

objects in space. Gaia also measured brightnesses and variability and those data were used to provide temperatures, gravitational parameters, stellar types and more for millions of stars. One of the key pieces of information Gaia provided was the distance to millions of stars.

Is your home internet down? Need to connect your laptop on the go? With a few taps, you can turn your smartphone into a source of internet that laptops, tablets, and other phones can use. This [article](#) from PCMag walks you through how to turn your smartphone into a wireless access point to connect you to the internet for both iPhone and Android phones.



Q.ANT

The world's first light-based chip offers 50x speed, and 30x efficiency over silicon-based chips, according to an [article](#) from Interesting Engineering. Q.ANT achieved this breakthrough by integrating its patented photonic chip technology onto a TFLN base. The company claims its photonic AI chip offers a massive increase in processing speed and energy efficiency compared to traditional silicon-based chips. This could potentially revolutionize

artificial intelligence (AI) data centers and high-performance computing (HPC).

Stargazers may soon get a rare, celestial treat. A star system 3,000 lightyears away is ready to go nova — and when it blows, it will be visible from Earth, according to an [article](#) from the New York Post. T Coronae Borealis, a.k.a. Blaze Star, only explodes once every 80 years, appearing as a new star in the night sky for around a week. The hydrogen from the red giant builds up around its partner, accumulating pressure and heat like air in a balloon — only when this balloon pops, it creates a thermonuclear explosion that can be seen across the galaxy. Out in space, the Blaze Star will shine thousands of times its original brightness, but to Earthlings it will appear as a new star in the sky about as bright as the North Star, known as Polaris.

A stunning discovery on Mars has revealed the longest organic molecules ever found on the planet—carbon chains that could resemble building blocks of life as we know it, according to an [article](#) from SciTechDaily. Preserved for billions of years in ancient Martian clay, these molecules were uncovered by NASA's Curiosity rover and could point to a more chemically complex past on the Red Planet.





Image by [Frank Rietsch](#) from [Pixabay](#)

A team of scientists warns that long-term exposure to Martian dust could harm future astronauts' lungs, thyroids, and more, according to an [article](#) from SciTechDaily. Packed with toxic compounds like silicates and perchlorates, the dust is small enough to bypass our body's defenses and enter the bloodstream. Drawing on rover data and meteorite analysis, researchers say now is the time to develop filters, supplements, and preventive measures before humans ever set foot on the Red Planet.

Four rocky planets much smaller than Earth orbit Barnard's Star, the next closest to ours after the three-star Alpha Centauri system. Barnard's is the nearest single star, according to an [article](#) from NASA. Barnard's Star, six light-years away, is notorious among astronomers for a history of false planet detections. But with the help of high-precision technology, the latest discovery — a family of four — appears to be solidly confirmed. The tiny size of the planets is also remarkable: Capturing evidence of small worlds at great

distance is a tall order, even using state-of-the-art instruments and observational techniques. These planets orbit their red-dwarf star much too closely to be habitable. The closest planet's "year" lasts a little more than two days; for the farthest planet, it is just shy of seven days. That likely makes them too hot to support life. Yet, their detection bodes well in the search for life beyond Earth. Scientists say small, rocky planets like ours are probably the best places to look for evidence of life as we know it. But so far they've been the most difficult to detect and characterize. High-precision radial velocity measurements, combined with more sharply focused techniques for extracting data, could open new windows into habitable, potentially life-bearing worlds.

A hormone-free male birth control pill is undergoing clinical testing for the first time ever, according to an [article](#) from ScienceAlert. The drug, called YCT-529, has performed incredibly well at limiting the production of sperm in mice and non-human primates, all while producing very few side effects. In male mice, the unique contraceptive kicks in within a month of use, reducing pregnancies in female mates by close to 100 percent. Male macaques require a higher dosage of YCT-529, but it also causes a rapid plummet in sperm count without severe side effects. Importantly, the animals soon regain their fertility when the medicine is stopped. The drug also causes no significant changes in three hormones important for sperm production: testosterone, FSH, or inhibin B.

 **FREE SOFTWARE**
FOUNDATION



Image by [FRANCO PATRIZIA](#) from [Pixabay](#)

Nitisinone, usually prescribed for metabolic disorders, kills mosquitoes when present in human blood, according to an [article](#) from Techno-Science.net. Researchers have explored a new approach to combat malaria using Nitisinone, a drug initially intended to treat rare metabolic diseases. This substance, by blocking an essential enzyme in mosquitoes, prevents them from digesting blood, leading to their rapid death. This discovery opens up prospects for a more sustainable and environmentally friendly method of controlling mosquito populations compared to traditional insecticides.

In a bid to tilt the cybersecurity battlefield in favor of defenders, Google has introduced Sec-Gemini v1, a new experimental AI model designed to help security teams identify threats, analyze incidents, and understand vulnerabilities faster and more accurately than before, according to an [article](#) from TechRepublic. Announced by the company's cybersecurity

research leads, Elie Burzstein and Marianna Tishchenko, Sec-Gemini v1 is the latest addition to Google's growing family of Gemini-powered tools — but this time, it is laser-focused on cybersecurity.

If I told you that your TV watches everything you do in the name of data collection and advertising, it likely wouldn't shock you, says an [article](#) from Lifehacker. It's 2025, after all; we're used to a general lack of privacy. Still, it's not cool, and it turns out you can stop it (even if your TV manufacturer has opted you into it). So, how do you stop your smart TV from tracking what you watch, so you can go back to the days of watching Netflix or playing video games in peace? You need to turn off ACR, short for automatic content recognition. It allows your smart TV to watch what you watch, identify what you watch, and use that information to both recommend new content and serve you more relevant ads. The article goes over how TV manufacturers "hide" the settings to turn ACR off. (I have this intrusive setting turned off on my smart TVs).



Google has released its April 2025 Android Security Bulletin, which includes patches for 62 vulnerabilities affecting Android devices,

according to an [article](#) from Lifehacker. Two of the fixes address critical zero-day flaws that may have been exploited in "limited, targeted" attacks, according to Google. Zero-days are security vulnerabilities that are exploited before the software developer can identify the flaw and issue a patch. The security update for April includes fixes for a range of issues, many of which elevation of privilege flaws.

Microsoft has detected a zero-day vulnerability in the Windows Common Log File System (CLFS) being exploited in the wild to deploy ransomware, according to an [article](#) from TechRepublic. Target industries include IT, real estate, finance, software, and retail, with companies based in the US, Spain, Venezuela, and Saudi Arabia. The vulnerability, tracked as CVE-2025-29824 and rated "important," is present in the CLFS kernel driver. It allows an attacker who already has standard user access to a system to escalate their local privileges. The individual can then use their privileged access for "widespread deployment and detonation of ransomware within an environment," according to a [blog post](#) by the Microsoft Threat Intelligence Center.

Microsoft's April 2025 Patch Tuesday includes security updates for 134 flaws, including one actively exploited zero-day vulnerability, according to an [article](#) from Bleeping Computer. This Patch Tuesday also fixes eleven "Critical" vulnerabilities, all remote code execution vulnerabilities. The number of bugs in each vulnerability category is listed here: 49 Elevation of Privilege Vulnerabilities, 9

Security Feature Bypass Vulnerabilities, 31 Remote Code Execution Vulnerabilities, 17 Information Disclosure Vulnerabilities, 14 Denial of Service Vulnerabilities, and 3 Spoofing Vulnerabilities. The above numbers do not include Mariner flaws and 13 Microsoft Edge vulnerabilities fixed earlier this month. Things that make you glad to be a Linux user!



Image by [Tumisu](#) from [Pixabay](#)

There's a lot of advice out there for proper password management: Each of your passwords should be strong and unique; use a secure manager to store your passwords; use two-factor authentication (2FA) to add an extra layer of security to your accounts, according to an [article](#) from Lifehacker. But there's another piece of advice that is held in the same regard as the others: Change your passwords often — perhaps once every three months. This habit is so emphasized, many companies and organizations will make you change your passwords multiple times a year in the name of security. The thing is, in all likelihood, this isn't actually doing anything to help your security. This idea that changing your passwords multiple times a year is a cornerstone of your security,

might be ingrained in some of you. After all, it's not new advice. As PCMag [examined](#), the practice goes back a long time: When security experts write about passwords, they often write about changing passwords, too. It's just the way the advice has been presented. But that's likely because it's anticipating and responding to bad security habits.

Google is hosting dozens of extensions in its Chrome Web Store that perform suspicious actions on the more than 4 million devices that have installed them and that their developers have taken pains to carefully conceal, according to an [article](#) from ArsTechnica. The extensions, which so far number at least 35, use the same code patterns, connect to some of the same servers, and require the same list of sensitive systems permissions, including the ability to interact with web traffic on all URLs visited, access cookies, manage browser tabs, and execute scripts.

Mobile applications are quietly attracting more and more malevolent attention — and for good reason, according to an [article](#) from TechNewsWorld. They contain a trove of private information about their users. In the iOS universe alone, 82.78%, or about 1.55 million apps, track private user data, according to the trends tracker [Exploding Topics](#). Mobile apps have also proven to be particularly vulnerable attack surfaces for cybercriminals. “Invisible” points of ingress and egress inside mobile apps can be compromised before legacy security tools even detect a breach. Those points include API calls, background syncing, and push notifications.



Google is fixing a long-standing privacy issue that, for [twenty] years, enabled websites to determine users' browsing history through the previously visited links, according to an [article](#) from Bleeping Computer. The problem arises from allowing sites to style links as 'visited,' meaning showing them as another color instead of the default blue if a user had previously clicked on them. The system displays this color change regardless of which site they were on when they clicked the link, allowing other sites to potentially use creative scripts that leak the user's browsing history.

Astronomers announced Thursday that they had detected the most promising “hints” of potential life on a planet beyond our solar system, though other scientists expressed skepticism, according to an [article](#) from CBS

News (and widely reported in multiple media outlets). There has been vigorous debate in scientific circles about whether the planet [K2-18b](#), which is 124 light years away in the Leo constellation, could be an ocean world capable of hosting microbial life, at least. Using the James Webb Space Telescope, a British-U.S. team of researchers detected signs of two chemicals in the planet's atmosphere long considered to be “biosignatures” indicating extraterrestrial life. On Earth, the chemicals dimethyl sulfide (DMS) and dimethyl disulfide are produced only by life, mostly microscopic marine algae called phytoplankton.

A new court ruling could change the dominant role Google has held in the digital advertising market since the release of AdWords in late 2000, according to an [article](#) from TechRepublic. On April 17, U.S. District Judge Leonie Brinkema ruled that Google illegally monopolized two markets: one for publisher ad servers and one for online ad exchanges. Antitrust investigators were unable to prove a monopoly in the advertiser [ad networks](#) market. Brinkema said Google is guilty of “willfully acquiring and maintaining monopoly power,” adding that “this exclusionary conduct substantially harmed Google's publisher customers, the competitive process, and, ultimately, consumers of information on the open web.”



*The PCLinuxOS Magazine
Created with Scribus*



In accordance with [Executive Order 14176](#), Declassification of Records Concerning the Assassinations of President John F. Kennedy, Senator Robert F. Kennedy, and the Reverend Dr. Martin Luther King, Jr., on January 23, 2025, **records relating to the assassination of Senator Robert F. Kennedy that have been released**, and will be available on the (U.S.) National Archives [website](#).

Earth rotates, the Sun rotates, the Milky Way rotates – and a new model suggests the entire Universe could be rotating, according to an [article](#) from ScienceAlert. If confirmed, it could ease a significant tension in cosmology. The Universe is expanding, but exactly how fast is a contentious question. Two different methods of measurement return two very different speeds – and as the measurements become more precise, each becomes more certain. This discrepancy is known as the Hubble tension, and it's reaching

crisis levels in physics. So for a new study, physicists in Hungary and the US added a small rotation to a model of the Universe – and this mathematical massage seemed to quickly ease the tension. “Much to our surprise, we found that our model with rotation resolves the paradox without contradicting current astronomical measurements,” [says](#) István Szapudi, an astronomer at the University of Hawaii.

Patients suffering from Parkinson's disease may soon benefit from a powerful treatment option: stem-cell transplants, according to an [article](#) from NPR. In a pair of small studies designed primarily to test safety, two teams of researchers found that stem cells transplanted into the brains of Parkinson's patients began producing the chemical messenger dopamine and appeared to ease symptoms like tremor, researchers [reported](#) in the journal Nature. The results indicate that “now we have the potential to really, really halt this disease in its tracks,” says Dr. Mya Schiess, a neurology professor at UTHealth Houston who was not involved in either study. The Food and Drug Administration has cleared one of the stem-cell treatments for a Phase 3 study, the last hurdle before approval.

Disclaimer

1. All the contents of the PCLinuxOS Magazine are only for general information and/or use. Such contents do not constitute advice and should not be relied upon in making (or refraining from making) any decision. Any specific advice or replies to queries in any part of the magazine is/are the person opinion of such experts/consultants/persons and are not subscribed to by the PCLinuxOS Magazine.
2. The information in the PCLinuxOS Magazine is provided on an "AS IS" basis, and all warranties, expressed or implied of any kind, regarding any matter pertaining to any information, advice or replies are disclaimed and excluded.
3. The PCLinuxOS Magazine and its associates shall not be liable, at any time, for damages (including, but not limited to, without limitation, damages of any kind) arising in contract, tort or otherwise, from the use of or inability to use the magazine, or any of its contents, or from any action taken (or refrained from being taken) as a result of using the magazine or any such contents or for any failure of performance, error, omission, interruption, deletion, defect, delay in operation or transmission, computer virus, communications line failure, theft or destruction or unauthorized access to, alteration of, or use of information contained on the magazine.
4. No representations, warranties or guarantees whatsoever are made as to the accuracy, adequacy, reliability, completeness, suitability, or applicability of the information to a particular situation.
5. Certain links on the magazine lead to resources located on servers maintained by third parties over whom the PCLinuxOS Magazine has no control or connection, business or otherwise. These sites are external to the PCLinuxOS Magazine and by visiting these, you are doing so of your own accord and assume all responsibility and liability for such action. Material Submitted by Users A majority of sections in the magazine contain materials submitted by users. The PCLinuxOS Magazine accepts no responsibility for the content, accuracy, conformity to applicable laws of such material.

Entire Agreement: These terms constitute the entire agreement between the parties with respect to the subject matter hereof and supersedes and replaces all prior or contemporaneous understandings or agreements, written or oral, regarding such subject matter.



PCLinuxOS Magazine Graphics Special Edition, Volumes 1 - 4

Uhleash your GIMP & Inkscape skills. Over 160 tutorials. Grab your FREE copy now!

Tip Top Tips: Fixing Filesystems Automatically After System Crash/Reset

Editor's Note: *Tip Top Tips* is a semi-monthly column in *The PCLinuxOS Magazine*. Periodically, we will feature – and possibly even expand upon – one tip from the PCLinuxOS forum. The magazine will not accept independent tip submissions specifically intended for inclusion in the Tip Top Tips column. Rather, if you have a tip, share it in the PCLinuxOS forum's "Tips & Tricks" section. Occasionally, we may run a "tip" posted elsewhere in the PCLinuxOS forum. Either way, share your tip in the forum, and it just may be selected for publication in *The PCLinuxOS Magazine*.

This month's [tip](#) comes from [kjpetrie](#).

Texstar has already suggested a remedy for this, but his method seems to require systemd, which in our case we have not got.

However, our current initscripts package already contains a mechanism for doing this, which needs just one small change to a configuration file to make it do a check. In `/etc/sysconfig/autofsck` change the line:

```
# Specify if we do automatic fsck.  
AUTOFSCK_DEF_CHECK=no
```

to

```
# Specify if we do automatic fsck.  
AUTOFSCK_DEF_CHECK=yes
```



If, and only if, your system is not properly shut down it will run `fsck` on boot before mounting partitions. I have just seen it in action after a hardware conflict reset my system. All four of my mounted partitions were checked in turn and corrected before my eyes as the system restarted. My home partition displayed a growing row of equal signs as the check proceeded.

The mechanism relies on `rc.sysinit` creating a hidden file called `./autofsck` on every boot. The `halt` script deletes that file. Hence, it will never exist until it is created on boot on a system

which ran `halt` to its conclusion. Before creating it, `rc.sysinit` checks if it does not already exist, and if it does, checks `/etc/sysconfig/autofsck` for instructions. By default, PCLinuxOS has the line set to no, but if you change it to yes you will get automatic checking when needed.

Discussion

Some users already had the setting enabled on their computers (sixte and myself were among those users). However, many other users did not already have this setting enabled (meaning it was set to "No").

The commands "`fsck.mode=force fsck.repair=yes`" appear to be silently ignored on PCLinuxOS, because we haven't got the program (systemd) which implements it.

Forum user **Stingray** provided a way for users to check to see when the last time `fsck` ran on their computer. Enter `tune2fs -l /dev/[drive] | grep checked` at a command line prompt, replacing [drive] with the drive device designation on your computer. If you're not sure what the drive designation is for your drive(s), simply open GParted and look at the drive designations there. Use those drive designations to complete the command and to get your answer. Remember: you're ONLY opening GParted to see what the drive designations are for your drive(s). Once you've written down the

drive designation(s), close GParted without doing anything else. You're only using GParted as a fact-finding mission tool.

While the ext4 filesystem (default in PCLinuxOS installations) has improved the stability for your filesystem, it's not necessarily bulletproof. If your computer does not shut down properly, or if you're forced to do a forced restart, you could end up with some damaged files from the system being unable to properly close those files. This tip definitely helps alleviate those fears, and helps fix any problems that may result from an unclean shutdown of your computer.



secure
private
simple-to-use
Sign up TODAY! pclosusers.com/services-signup.php

Screenshot Showcase



Posted by minimouse, on April 1, 2025, running Mate.



Linux DocsLinux
Man Pages



Like us on Facebook!

PCLinuxOS Magazine

PCLinuxOS Fan Club



Wiki Pick: Numlock On At Login

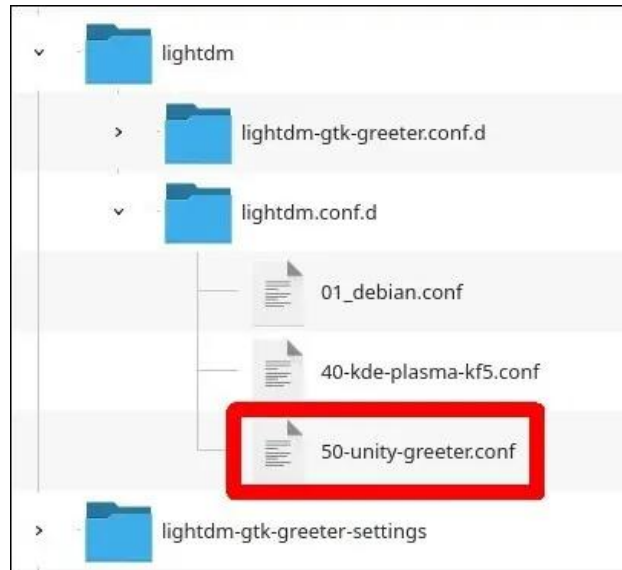
by David Marshall (CoreLite)

Editor's Note: Wiki Pick is a new monthly column highlighting one article from the PCLinuxOS Knowledge Base [Wiki](#) every month. Whenever possible (and when known), we'll attribute the Wiki Pick article to the PCLinuxOS user who made the Wiki post. The Wiki cannot survive and thrive without the efforts of PCLinuxOS members contributing and keeping it updated. So, visit and contribute to YOUR PCLinuxOS Knowledge Base Wiki!

This is one of those irritating little things that isn't broken. If you use a lot of numbers in your logon password, not being able to use the number keypad at logon is a muscle memory problem. This will show you the method of getting numlock to be on at the login screen.

If you want numlock on at the boot up log in screen so that you can use your number keypad, you need to install numlockx and configure it using the following steps.

1. Log in to root.
2. Open **Synaptic** and install **numlockx**.
3. Create a text file named **50-unity-greeter.conf** in **/usr/share/lightdm/lightdm.conf.d/**



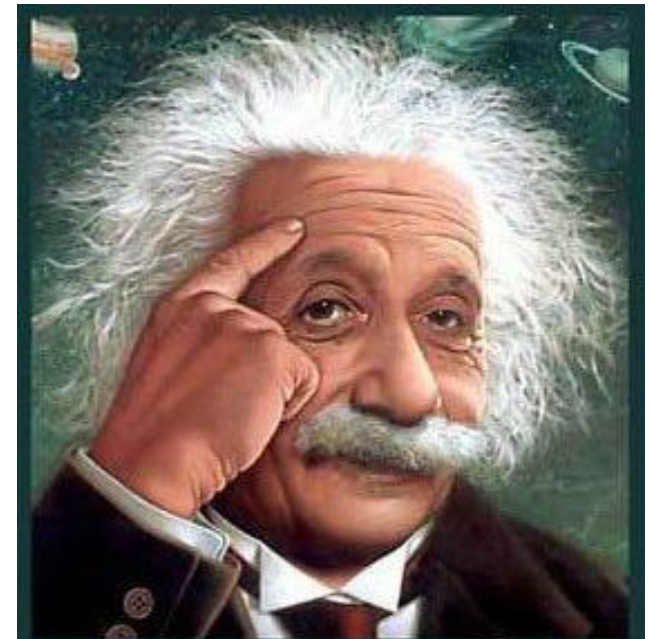
4. Open **50-unity-greeter.conf** in a text editor.
5. Copy and paste the following code in to the **50-unity-greeter.conf** file:

```
[Seat:*]
greeter-session=unity-greeter
greeter-setup-script=/usr/bin/numlockx on
```

6. Save your changes.
7. Close your text editor and any other open applications and reboot.

You can now use your number keypad when you log in.

You can view the original Wiki page [here](#).



*It's easier than $E=mc^2$
It's elemental
It's light years ahead
It's a wise choice
It's Radically Simple
It's ...*

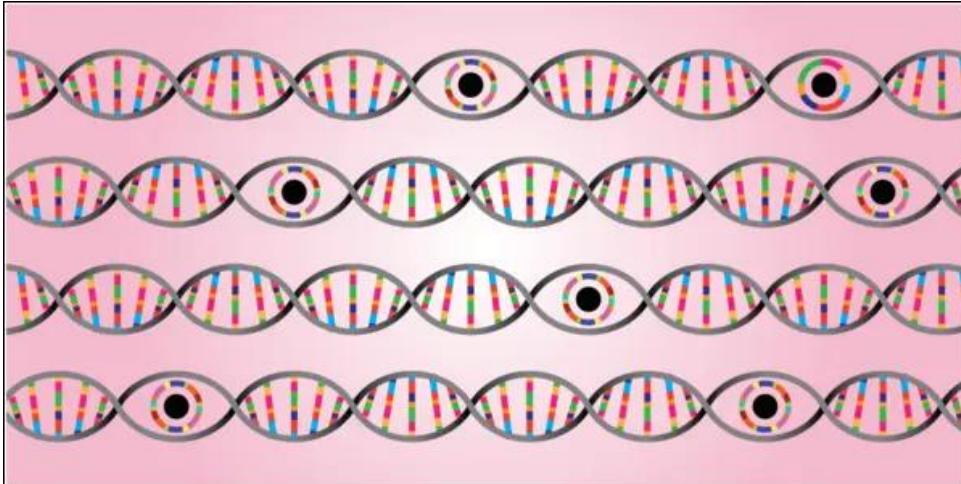


How To Delete Your 23andMe Data

by **Thorin Klosowski**

Electronic Frontier Foundation

Reprinted under Creative Commons [License](#)

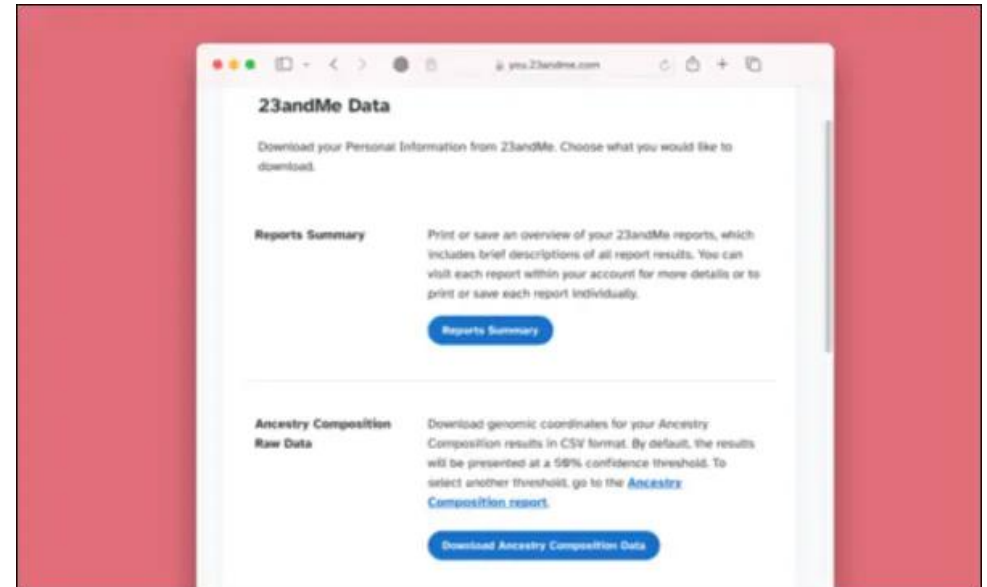


This week, the genetic testing company [23andMe filed for bankruptcy](#), which means the genetic data the company collected on millions of users is now up for sale. If you do not want your data included in any potential sale, it's a good time to ask the company to delete it.

When the company first announced it was considering a sale, we highlighted many of the [potential issues](#), including selling that data to companies with poor security practices or direct links to law enforcement. With this bankruptcy, the concerns we expressed last year remain the same. It is unclear what will happen with your genetic data if 23andMe finds a buyer, and that uncertainty is a clear indication that you should consider deleting your data. California attorney general Rob Bonta [agrees](#).

 **FREE SOFTWARE**
FOUNDATION

First: Download Your Data



Before you delete your account, you may want to download the data for your own uses. If you do so, be sure to store it securely. To download your data:

1. Log into your 23andMe account and click your username, then click “Settings.”
2. Scroll down to the bottom where it says “23andMe Data” and click “View.”
3. Here, you'll find the option to download various parts of your 23andMe data. The most important ones to consider are:
 - 3.1 The “Reports Summary” includes details like the “Wellness Reports,” “Ancestry Reports,” and “Traits Reports.”

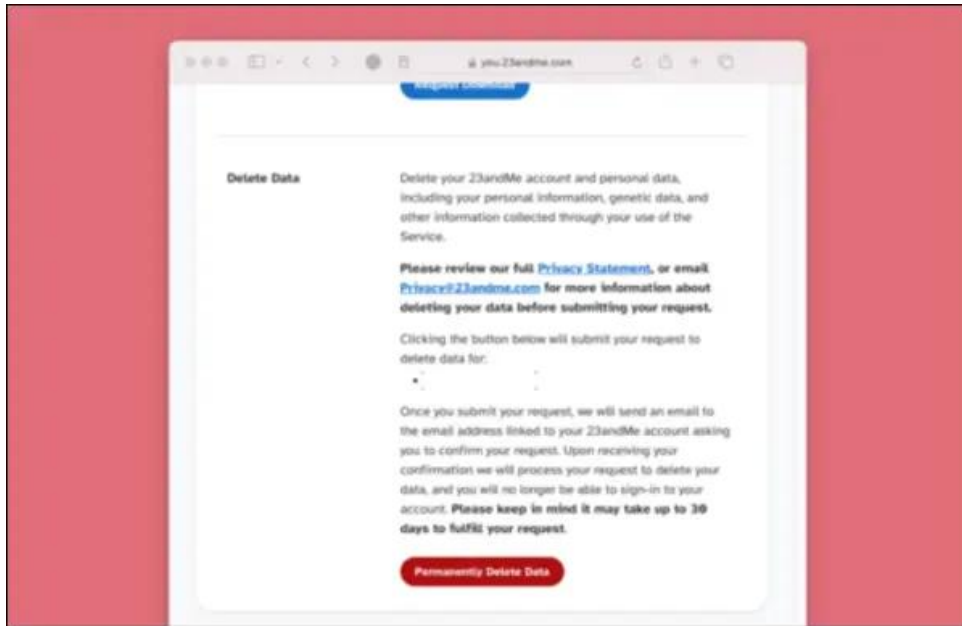
3.2 The “Ancestry Composition Raw Data” the company’s interpretation of your raw genetic data.

3.3 If you were using the DNA Relatives feature, the “Family Tree Data” includes all the information about your relatives. Based on the descriptions of the data we’ve seen, this sounds like the data the bad actors collected.

3.4 You can also download the “Raw data,” which is the uninterpreted version of your DNA.

There are other types of data you can download on this page, though much of it will not be of use to you without special software. But there’s no harm in downloading it all.

How to Delete Your Data



Finally, you can delete your data and revoke consent for research. While it doesn’t make this clear on the deletion page, this also [authorizes](#) the company to destroy your DNA sample, if you hadn’t already asked them to

do so. You can also make this request more explicit if you want in the [Account preferences section](#) page.

If you’re still on the page to download your data from the steps above, you can skip to step three. Otherwise:

1. Click your username, then click “Settings.”
2. Scroll down to the bottom where it says “23andMe Data” and click “View.”
3. Scroll down to the bottom of this page, and click “Permanently Delete Data.”
4. You should get a message stating that 23andMe received the request but you need to confirm by clicking a link sent to your email.
5. Head to your email account associated with your 23andMe account to find the email titled “23andMe Delete Account Request.” Click the “Permanently Delete All Records” button at the bottom of the email, and you will be taken to a page that will say “Your data is being deleted” (You may need to log in again, if you logged out).

23andMe should give every user a real choice to say “no” to a data transfer in this bankruptcy and ensure that any buyer makes real privacy commitments. Other consumer genetic genealogy companies should proactively take these steps as well. Our DNA contains our entire genetic makeup. It can reveal where our ancestors came from, who we are related to, our physical characteristics, and whether we are likely to get genetically determined diseases. Even if you don’t add your own DNA to a private database, a relative could make that choice for you by adding their own.

This incident is an example of why this matters, and how certain features that may seem useful in the moment can be weaponized in novel ways. A bankruptcy should not result in our data getting shuffled off to the highest bidder without our input or a guarantee of real protections.

PCLinuxOS Recipe Corner Bonus



French Onion Beef and Noodles

Serves: 6

INGREDIENTS:

2 tablespoons Olive Oil
1 pound Beef Stew Meat
1 teaspoon Onion Powder
1 teaspoon Garlic Powder
Salt & Pepper, to taste
1 can (10.5 ounces) French Onion Soup
3 cups Beef Broth
12 ounces Egg Noodles
½ cup Sour Cream
¼ cup Parmesan Cheese
1 cup French Fried Onions

DIRECTIONS:

Heat the Oil: In a large pot, heat olive oil over medium-high heat.

Sear the Beef: Add beef stew meat and season with onion powder, garlic powder, salt, and pepper. Sauté for 3-5 minutes until beef is seared on all sides.

Simmer with Soup and Broth: Pour in French onion soup and beef broth. Bring to a simmer, then let the beef cook on low for 10 minutes.

Cook the Noodles: Add egg noodles to the pot and continue to simmer for an additional 10 minutes, stirring occasionally, until noodles are tender.

Add Dairy: Remove the pot from heat. Stir in sour cream and Parmesan cheese until well combined.

Serve: Sprinkle with French fried onions before serving.

NOTES:

Enjoy this flavorful dish as a comforting main course.

Pair with a crisp green salad or steamed vegetables for a balanced meal.

NUTRITION:

Calories: 471 Carbs: 31g Sodium: 536mg
Fiber: 2g Protein: 34g

DESTINATION LINUX
Linux is Our Passion



FSF FREE SOFTWARE
FOUNDATION

PCLinuxOS Puzzled Partitions

		5	6	2			3	
				3	8		4	
3	9		1			8		
	8			1	4			6
	3							5
5	1	8		9				
		6	8			1	7	

SUDOKU RULES: There is only one valid solution to each Sudoku puzzle. The only way the puzzle can be considered solved correctly is when all 81 boxes contain numbers and the other Sudoku rules have been followed.

When you start a game of Sudoku, some blocks will be prefilled for you. You cannot change these numbers in the course of the game.

Each column must contain all of the numbers 1 through 9 and no two numbers in the same column of a Sudoku puzzle can be the same. Each row must contain all of the numbers 1 through 9 and no two numbers in the same row of a Sudoku puzzle can be the same.

Each block must contain all of the numbers 1 through 9 and no two numbers in the same block of a Sudoku puzzle can be the same.



SCRAPPLER RULES:

1. Follow the rules of Scrabble®. You can view them [here](#). You have seven (7) letter tiles with which to make as long of a word as you possibly can. Words are based on the English language. Non-English language words are NOT allowed.
2. Red letters are scored double points. Green letters are scored triple points.
3. Add up the score of all the letters that you used. Unused letters are not scored. For red or green letters, apply the multiplier when tallying up your score. Next, apply any additional scoring multipliers, such as double or triple word score.
4. An additional 50 points is added for using all seven (7) of your tiles in a set to make your word. You will not necessarily be able to use all seven (7) of the letters in your set to form a "legal" word.
5. In case you are having difficulty seeing the point value on the letter tiles, here is a list of how they are scored:
 0 points: 2 blank tiles
 1 point: E, A, I, O, N, R, T, L, S, U
 2 points: D, G
 3 points: B, C, M, P
 4 points: F, H, V, W, Y
 5 points: K
 8 points: J, X
 10 points: Q, Z
6. Optionally, a time limit of 60 minutes should apply to the game, averaging to 12 minutes per letter tile set.
7. Have fun! It's only a game!

R₁ U₁ P₃ L₁ A₁ E₁ G₂

— — — — — — —

L₁ U₁ L₁ C₃ R₁ D₂ O₁

— — — — — — —

Triple Word

O₁ O₁ A₁ L₁ B₃ H₄ N₁

— — — — — — —

A₁ R₁ R₁ A₁ A₁ O₁ U₁

— — — — — — —

Double Word

M₃ U₁ U₁ U₁ S₁ L₁ C₃

— — — — — — —

Possible score 222, average score 155.

Download Puzzle Solutions Here

May 2025 Word Find

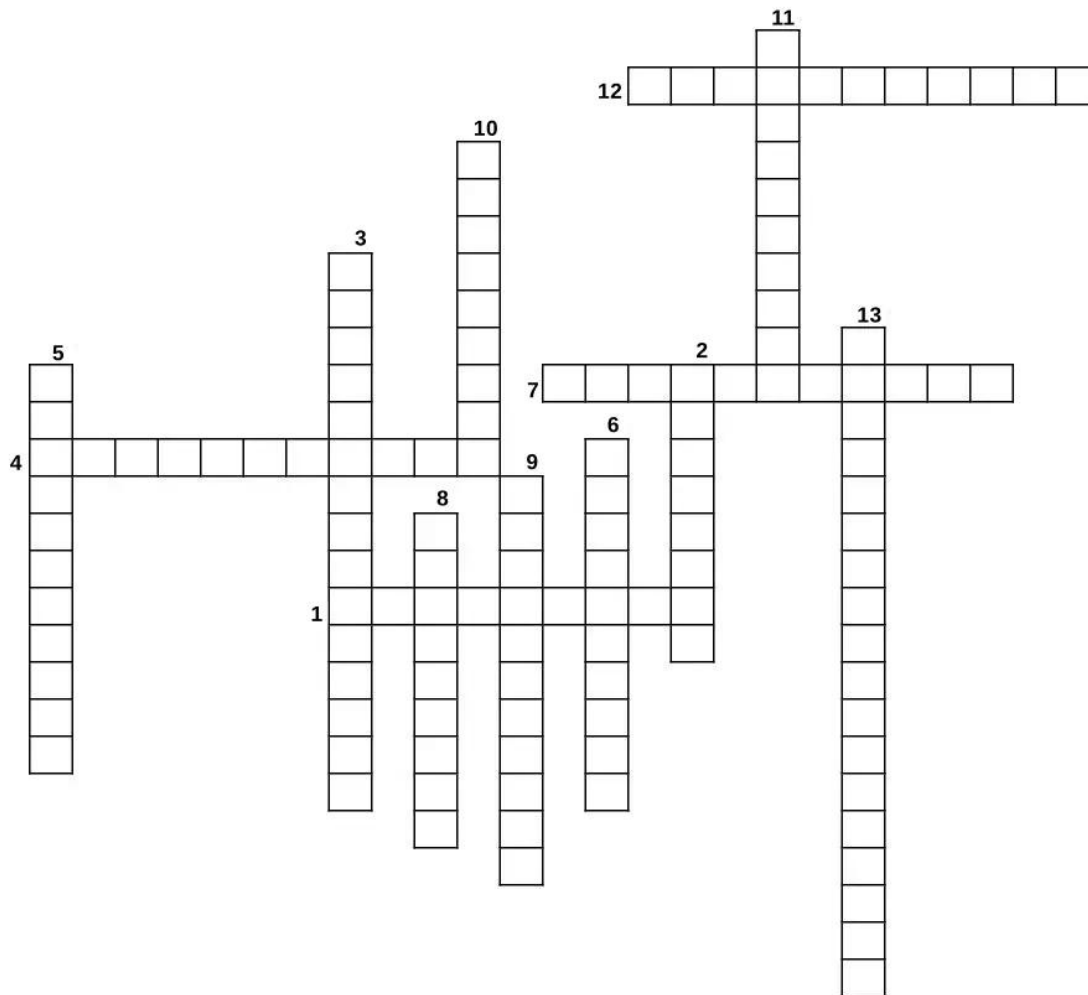
Weather

T U B J K J S T R A T O C U M U L U S V J P M P Q U O F E T
 V A N V S J R T P T M S N J C J V F A F K Y A C N D T V L E
 I W A T M O S P H E R I C P R E S S U R E J U V E U V W I L
 Y G O L O R O E T E M B T J L S J W N R O M S M G O M A P C
 H G Z M T H A F O H H E S A P S V F T B U R F Q L L H Y O Y
 C H I N O O K W I N D X T A Y N G K K L P X U A J C A H D C
 G H N Z P W C A M J A U O Z F S I D O M A K V A U S H S A C
 R L I B W D G U L S A P V P Z A S N S V I I I B G U T E N I
 E G Q G R E T E M O R G Y H A C I H A B O O B C N E D L R G
 E W E E B A M I Q U R L H M W M E I T E G E X Z F L A A O O
 N A O O H Y L W F B L W W B B G O Y P M E K I L A I D C T L
 H L N A W B D J R E H U N U Y Q X K X C R T T C P P D S E O
 O L S H L M A M M A T U S C L O U D G I J V S Q P O R D P R
 U C T Y Q Q N B Y I F C U M O J H R K R E K R S R G K N O D
 S L N T E K N O A T U S D J V B Q U A R R A U A D Y B I R Y
 E O I H R A C S R G J N A O Z E Q M R I E L B E U H G W K H
 E U M H I F U E O N I G R L L K Y J D F H H O X O H N T N F
 F D B J F Q M Q H T T M Y Q T D G G A O P G R V L Y O R H Z
 F G O S S X U T P S A Y Z M K O R K A R S Y C Q C D I O J Z
 E H S D O T L F C R S H L A A A S U U M O C A A C R L F M W
 C A T N M U U Q M U C E A E U N V T M X T J M P I O E U F H
 T A R A L S S T K B A H J P A K E H R S A K G A H S H A H X
 K B A B E F H E O O L G E E T S A M I A R W P A P P R E J K
 A T T R T W F O O R E L A Z Y W T M O G T K G G A H A B B M
 U T U E S L O Q D C S N R T A X F E L M S U W I R E P G D S
 H S S D G O A A Y I O D T F Q B L W R P E N S Z G R T H D W
 G J U E R W G K P M B I Y Z M Y R N Q L V T V V O E Y U V O
 H J D E C C Y L U X W S X U F H O T N Q I A E O R J R J W M
 C I K F T R O P O S P H E R E T T E F U M E S R O Y Q T W G
 J Y E B O U G E B A R O M E T R I C P R E S S U R E L N N P

ALTOCUMULUS	ALTOSTRATUS
ANEMOMETER	
ATMOSPHERIC PRESSURE	AURORA
BAROMETRIC PRESSURE	
BEAUFORT WIND SCALE	
CHINOOK WIND	
CIRRIFORM	CUMULONIMBUS
CUMULUS	DOLDRUMS
EASTERLIES	FEEDER BANDS
FUJITA SCALE	GRAUPEL
GREENHOUSE EFFECT	HABOOB
HYDROLOGIC CYCLE	
HYDROSPHERE	
HYGROMETER	MACROBURST
MAMMATUS CLOUD	
METEOROLOGY	
MICROBURST	
NIMBOSTRATUS	
OROGRAPHIC CLOUD	
PARHELION	
PILEUS CLOUD	ROPE TORNADO
ST ELMO'S FIRE	STRATOCUMULUS
STRATOSPHERE	TROPOSPHERE
WALL CLOUD	

[Download Puzzle Solutions Here](#)

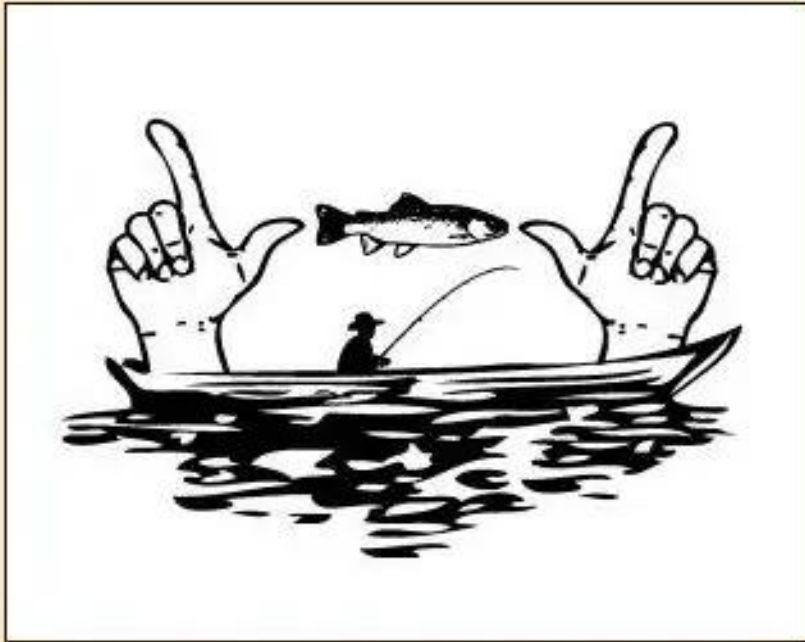
May 2025 Crossword Weather



1. A type of cloud that is thin and wispy in appearance, typically found at high altitudes.
2. A nautical term that refers to the belt around the Earth near the equator where sailing ships sometimes get stuck on windless waters.
3. Also known as the water cycle, it is the continuous movement of water on, above, and below the Earth's surface.
4. An accessory cloud of small horizontal extent, in the form of a cap or hood above the top or attached to the upper part of another cloud.
5. Tornado whose appearance looks very long and thin, but is capable of considerable damage.
6. An instrument which measures the humidity of air or some other gas.
7. Lines of low-level clouds that move into the updraft region of a thunderstorm.
8. A bright spot sometimes appearing at either side of the sun, often on a luminous ring or halo, caused by the refraction and reflection of sunlight by ice crystals suspended in the earth's atmosphere.
9. A system used to measure the intensity of tornadoes based on the damage they cause to buildings and vegetation.
10. A large, persistent, and often abrupt lowering of cloud that develops beneath the surrounding base of a cumulonimbus cloud and from which tornadoes sometimes form.
11. An instrument for measuring and recording the speed of the wind.
12. A warm, dry wind descending the eastern slopes of the Rocky Mountains, primarily in winter.
13. The amount of force per area exerted by air in the atmosphere against humans and other objects on earth.

[Download Puzzle Solutions Here](#)

Mixed-Up-Meme Scrambler



IXTYS

 _ _

FASHE

 _ _

ENDTOE

 _ _ _

SAURES

 _ _

When he told them about his whopper,
his pals said it

" _ _ _ _ _ " _ _ _ _ _

[Download Puzzle Solutions Here](#)

More Screenshot Showcase



Posted by luikki, on April 1, 2025, running KDE.



Posted by hunter0one, on April 2, 2025, running KDE.



Posted by francesco_bat, on April 21, 2025, running icewm.



Posted by astronaut, on April 9, 2025, running openbox.