UNINSTALLING FIREFOX ADDONS

by John Krout, PATACS member

At the July 20, 2019 meeting of PATACS and OLLI OPCUG in Fairfax City, a question was raised pertaining to a recent Washington Post article reporting that many Firefox and Chrome browser addons were scretly reporting browser use. This has been known to be a issue with some browser cookies for quite some time, but browsers also support other types of addons, such as Adobe Flash for media playback and ad blockers. Browser usage reporting means that some addons are ***spyware***, noting and reporting the web sites you visit and possibly data you enter on Web pages such as your name, email address and physical address, account IDs and passwords, et cetera, without asking your permission to do such reporting.

This is hardly an abstract concern. I place orders on my stock broker web site involving an investment portfolio that is now worth over a quarter of a million dollars. If my ID and password is reported to some bad apple, and that bad apple uses the info to liquidate that account, I would be unable to retire anytime soon.

At the meetng, Paul Howard, PATACS President, asked members to look into this matter. Here is what I learned.

Note, I developed this guide and captured images from Firefox version 68.0.1 (64-bit). If you use an older Firefox version, install the latest version to take advantage of the settings shown below.

WHAT IS AN ADDON?

Web browsers provide various ways for third parties to add capabilities to the browsers. This is done by adding software to your computer. This could be either Java software to be executed by the Java Virtual Machine of the browser, or an executable library. Some of those capabiities help you, some help the addon publisher learn about you, and some do both.

Firefox itself identifies three types of addons: extensions, plug-ins, and themes. Additionally, I suggest that it is important to view cookies as addons.

COOKIES

Cookies are relatively small data structures that are stored in your browser at the request of a web site. Many, if not most, include Java code that can be executed by the browser without your knowledge or permission.

Originally cookies were created for purposes such as retaining your login credentials, ID and password, for a frequently used web site. You might find that useful for your email provider's site, so you do not have to log in every time you visit that site. In the past I have used that behavior, for instance, for access to my accounts on two email account sites, the Geocaching.com site and on Amazon.

Retailer web sites such as Amazon also use a cookie as your shopping cart. The cookie in your browser remembers the products you have decided to purchase. That way, when you finally choose to pay for your purchases, the cookie tells Amazon what you want, so that Amazon can add up the prices and figure out the shipping cost and delivery dates.

Obviously, those cookies can help you. However, you and many other people are never told that cookies are used to accomplish those useful things. At least not until you read this article.

Cookies exist because the Web was designed to be ***connectionless***, meaning that the Web server does not have any means on the server side to remember that your browser, or any other browser, is using the Web server.

Cookies on your computer provide that memory.

Cookies are usually installed without your express consent or knowledge. These days, cookies can include Java software to report a great deal of what you do with your browser to the cookie publisher. Usually the aim is to make money selling that info to advertisers, again without your consent or knowledge.

Clearly, cookies have a capability to communicate over the Internet. And cookies are now widespread. After three weeks of ownership and occasional use of my new desktop computer and the Firefox browser, I had over 600 Kilobytes of cookies on my hard drive. I told Firefox to prevent future cookie storage, but the 600K was installed before I told Firefox to do that.

HOW TO PREVENT COOKIES FROM BEING INSTALLED PERMANENTLY

You can set Firefox to permanently prevent cookies from being installed. For some Web sites, this setting can literally prevent you from using the site. For instance, as mentioned above, while using Amazon, your Shopping Cart is literally a cookie containing the identification of each product you have chosen to purchase. If you prevent Amazon from creating such a cookie, then you cannot make a purchase on Amazon. Most retail web sites use the same approach.

So, Firefox provides another way, a useful compromise. You can tell Firefox to allow cookies to be created, but then delete the cookies each time you close your Web browser. That way the retailer cookies persist only as long as you need them, meaning while you are using the retailer web site. This Firefox configuration is known as **Permanent Private Browsing.**

Using this Firefox configuration option does mean that sites such as Amazon and your email provider will not automatically recognize you when you open the browser and go to the site. You will be forced to log in every time you visit such a site. This is the price to be paid for no permanent cookies.

Firefox also provides a detailed explanation of what Private browsing does not save on your computer. Here is that explanation:

What does Private Browsing not save?

Visited pages: No pages will be added to the list of sites in the History menu, the Library window's history list, or in the address bar drop-down list. [the consequence of this is that the browser will not complete URLs when you start typing them]

Form and Search Bar entries: Nothing you enter into text boxes on web pages or the Search bar will be saved for Form autocomplete [This means that you cannot expect a form including street address, state and zip code to be completed by the browser. You must do it yourself].

Passwords: No new passwords will be saved.

Download List entries: No files you download will be listed in the Downloads Window after you turn off Private Browsing.

Cookies: Cookies store information about websites you visit such as site preferences, login status, and data used by plugins like Adobe Flash. Cookies can also be used by third parties to track you across websites. See How do I turn on the Do Not Track feature? for more information about tracking. Cookies set in private windows are held temporarily in memory, separate from regular window cookies, and discarded at the end of your private session (after the last private window is closed).

Cached Web Content and Offline Web Content and User Data: No temporary Internet files (cached files) or files that websites save for offline use will be saved.

<end of documentation shard>

Here is how you can configure that Permanent Private Browsing behavior in Firefox.

1. Open a new Firefox window. Find the three horizontal lines in the upper right corner. Those three lines are the button for opening the Firefox main menu.

Illustration 1. Firefox home page with Menu button

2. Click on the three lines. The Firefox main menu opens, as shown below.

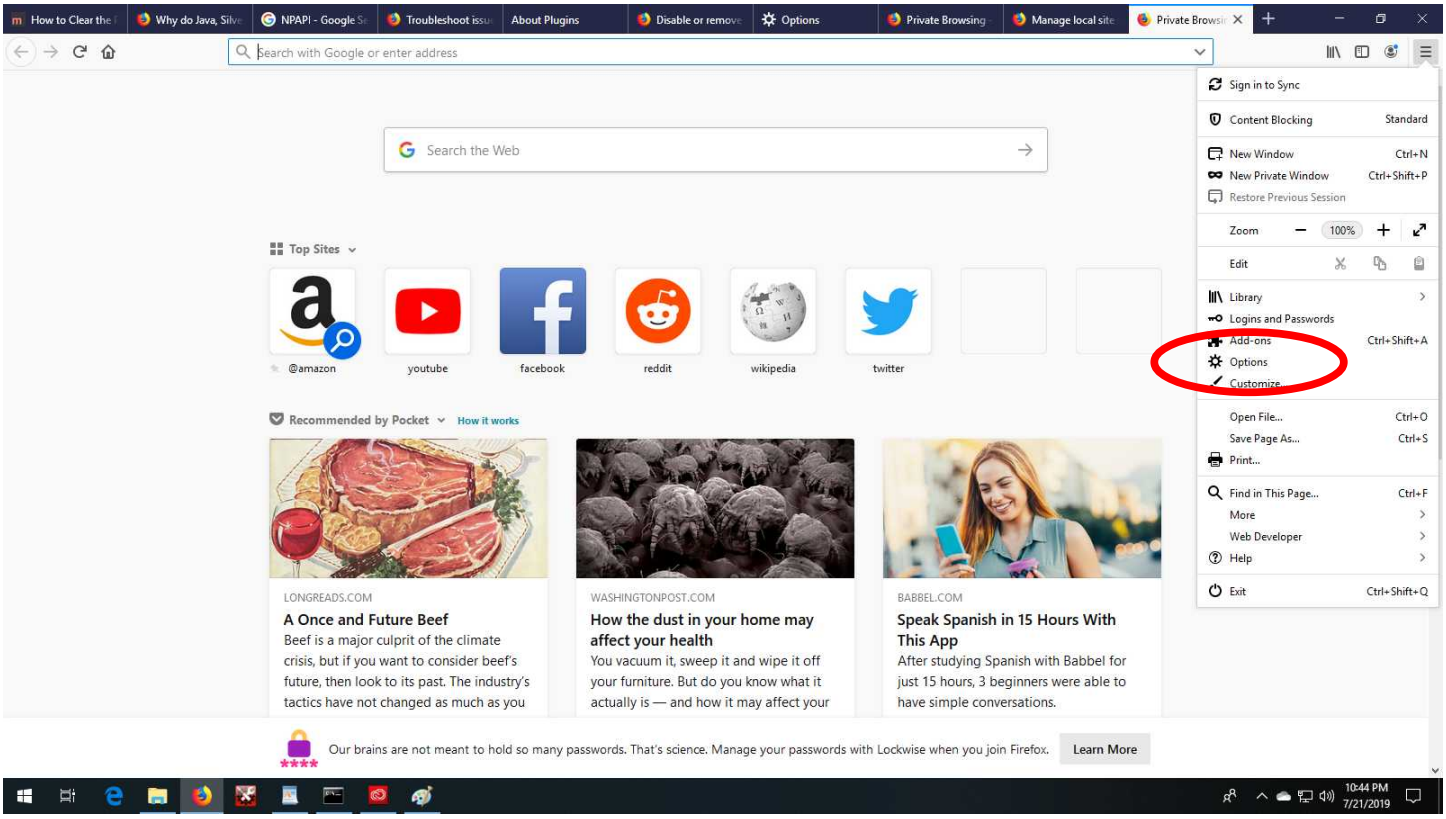

Illustration 2. Firefox with main menu displayed and Options choice circled

3. In the menu, click on Options. In the illustration above, the Options choice is circled. That choice causes the tab to load the Options page as shown below.

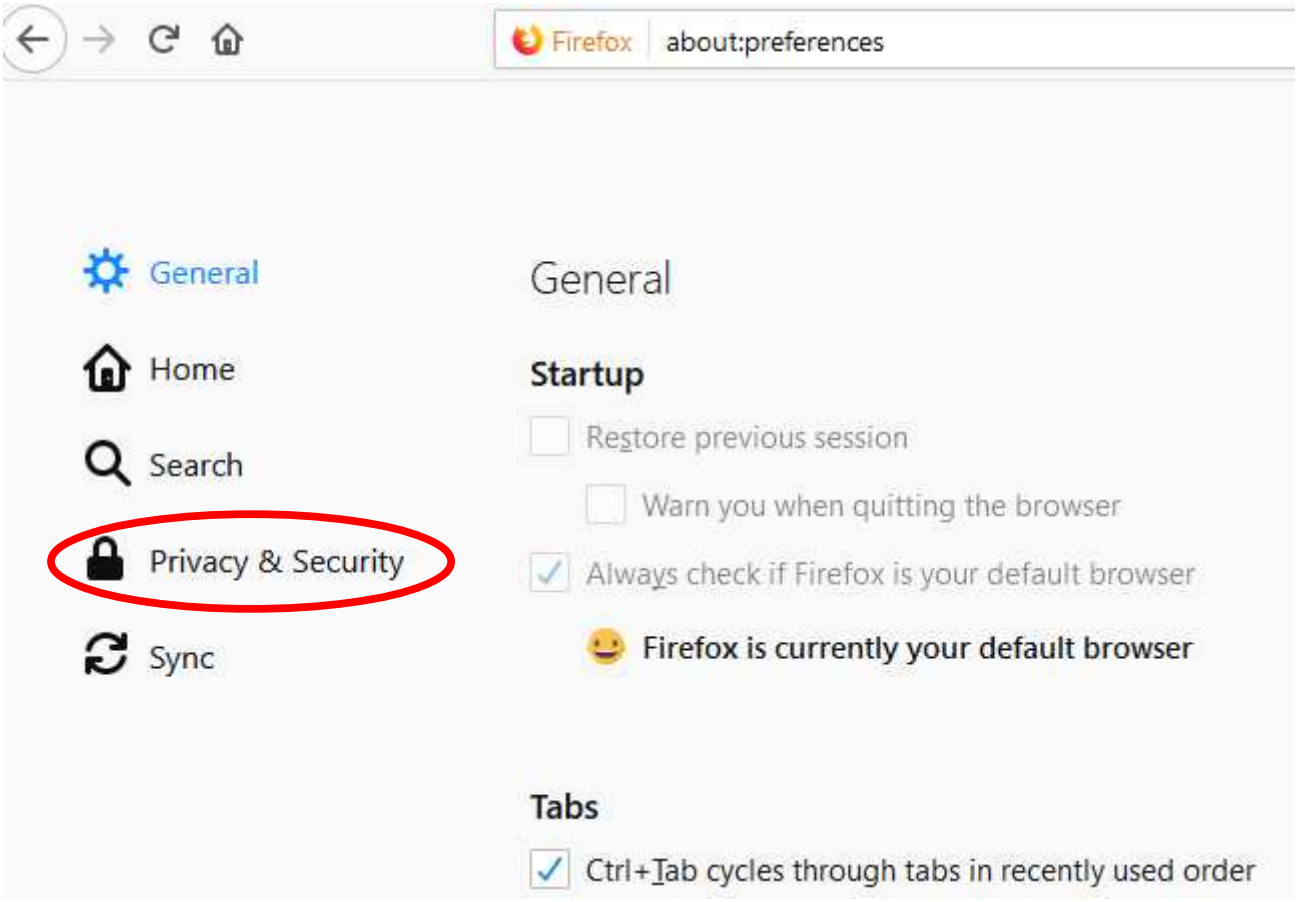

Illustration 3. Firefox Options page with left hand menu item Privacy & Security circled.

4. In the Options page, on the left side, click on the Privacy & Security link. That link is circled in the illustration above. A new page appears as shown below.

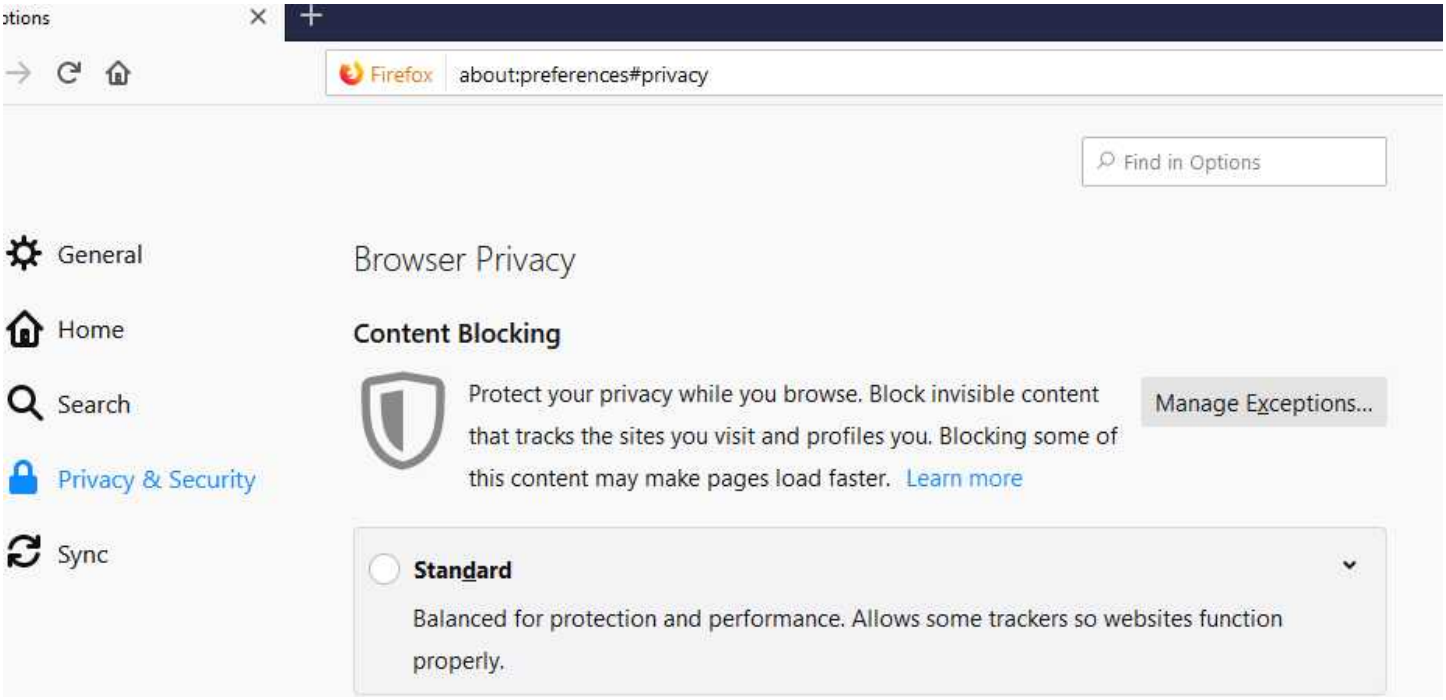

Illustration 4. Top of Firefox Privacy & Security page.

5. The page is long. In that page, scroll down to the History heading.

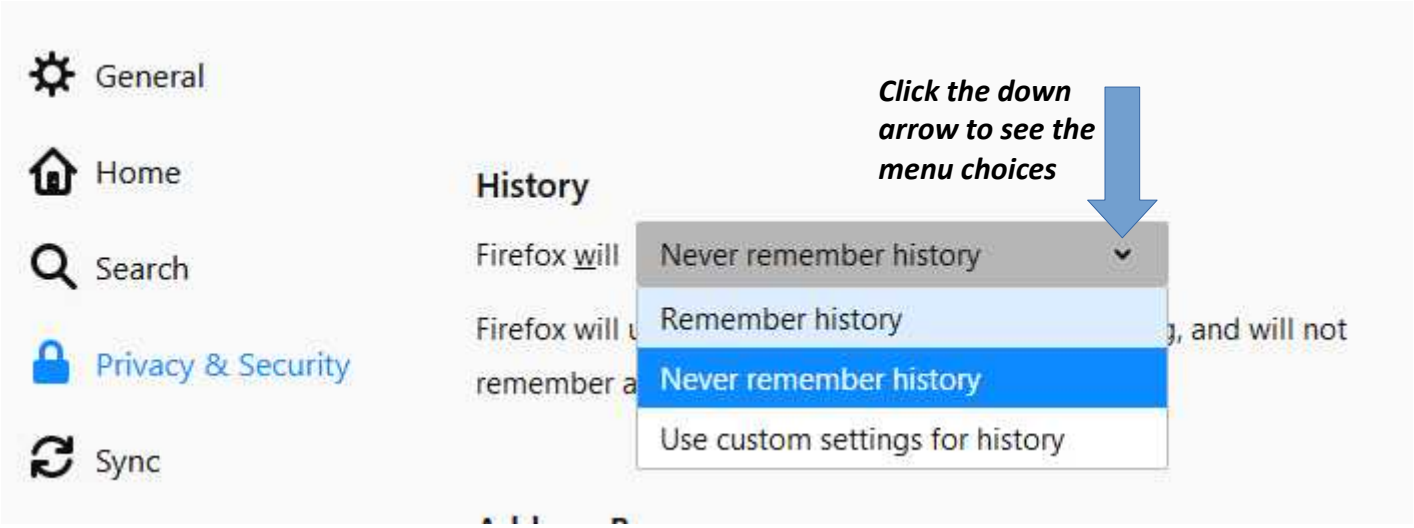

Illustration 5. Firefox Privacy & Security page History heading with dropdown menu displayed.

6. Below the **History** heading, the words **Firefox will** are followed by a dropdown menu. Click on the down-arrow symbol to see the choices. Choose NEVER REMEMBER HISTORY to establish Permanent Private Browsing.

Private browsing is not a global cure for all the adverse effects of nasty cookies. If you are forced to download any nasty cookies while using Private Browsing mode, then those will report whatever you do with your browser until you shut down the browser. Shutting down does not mean iconize the browser, shutting down means terminating the browser application, either by tapping the X in the upper right corner of the browser window, or (in Windows) by tapping the ALT-F4 key combination while the browser is the selected application.

Obviously, shutting down the browser frequently minimizes the scope of the reports made by nasty cookies.

WAYS TO BLOCK THOSE NASTY COOKIES IMMEDIATELY

There are other settings at the top of the Privacy & Security page that will enable the browser to block those nasty cookies while allowing more useful cookies to do their work while the browser remains running. See illustration 4 above: Under Content Blocking, there are options for Standard and for Strict blocking. I chose the Strict option, and that option has not broken any of my frequently visited Web sites thus far.

This tracking cookie blocking capability is an ongoing battle between the browser publishers and increasing sly and subtle cookie developers. Even the Strict setting is never going to be 100% victorious. Below you will read about an Extension that attempts to do even more than what the Strict blocking accomplishes.

OTHER ADDONS

As mentioned above, Firefox's own help pages identify three categories of Firefox add-ins: plug-ins, extensions, and themes.

A **theme** is simply a way of managing the browser colors and control layout, and embedding a favorite photo as a background image. I do not know if themes have any capability to communicate over the internet. As of now, July 2019, I do not think so.

FIREFOX PLUG-INS

I had to research the definition of a Firefox plug-in. Here is what Firefox documentation says:

A plug-in is a piece of software that manages Internet content that Firefox is not designed to process. These usually include patented formats for video, audio, online games, presentations, and more. Plug-ins are created and distributed by other companies.

Here are examples, also from Firefox documentation:

Adobe Flash: Flash Plugin - Keep it up to date and troubleshoot problems

Java: Use the Java plugin to view interactive content on websites

QuickTime: Use the QuickTime plugin to play audio and video [this is an Apple video player]

Silverlight: Use the Silverlight plugin to play audio and video [this is a Windows video player]

Adobe Acrobat: Use Adobe Reader to view PDF files in Firefox

Windows Media: Play Windows Media files in Firefox with the Windows Media plugin

In short, the examples primarily cover media display capabilities. I admit that the description of Java as a plug-in has me a bit baffled. I thought Java was standard in browsers, not a plug-in.

I am sure that the plug-ins all report some aspect of their use to their publishers, especially including crash reports. This makes sense. However, it probably means the publishers have at least considered adding a wider range of tracking capability to each plug-in.

Firefox documentation also notes that Firefox is eliminating support for most plug-ins. Here is what Firefox says on the topic:

Beginning in Firefox version 52 released March 7, 2017, installed NPAPI plugins are no longer supported in Firefox, except

for Adobe Flash.

<end of documentation shard>

NPAPI stands for Netscape Plugin Application Programming Interface. This originated many years ago with the Netscape web browsers.

I have to admit that watching YouTube and Netflix using a browser is valuable. So I wondered why the NPAPI is being dropped, and what is being done to support media playback instead of using the NPAPI plug-ins.

Further down on the same documentaton page, Firefox says that users frequently found that plug-ins slowed down Firefox or crashed Firefox. I suspect this adverse effect is the motivation for eliminating plug-ins. Firefox and partners are working to replace the NPAPI with what Firefox describes as Web API plug-ins.

FIREFOX EXTENSIONS

Likewise, I examined Firefox decoumentation to find a definition of extensions. Here is their defintion:

Extensions add new features to Firefox or modify existing ones. There are extensions that allow you to block advertisements, download videos from websites, integrate Firefox with websites like Facebook or Twitter, and add features included in other browsers, such as translators.

<end of documentation shard>

IDENTIFYING AND REMOVING ADDONS

This is a subject whenich Firefox does not document in a very straightforward manner.

Nonetheless, there is a very simple way in Firefox to list all the addins by type.

In the Firefox URL bar, type **about:addons** and tap the Enter key.

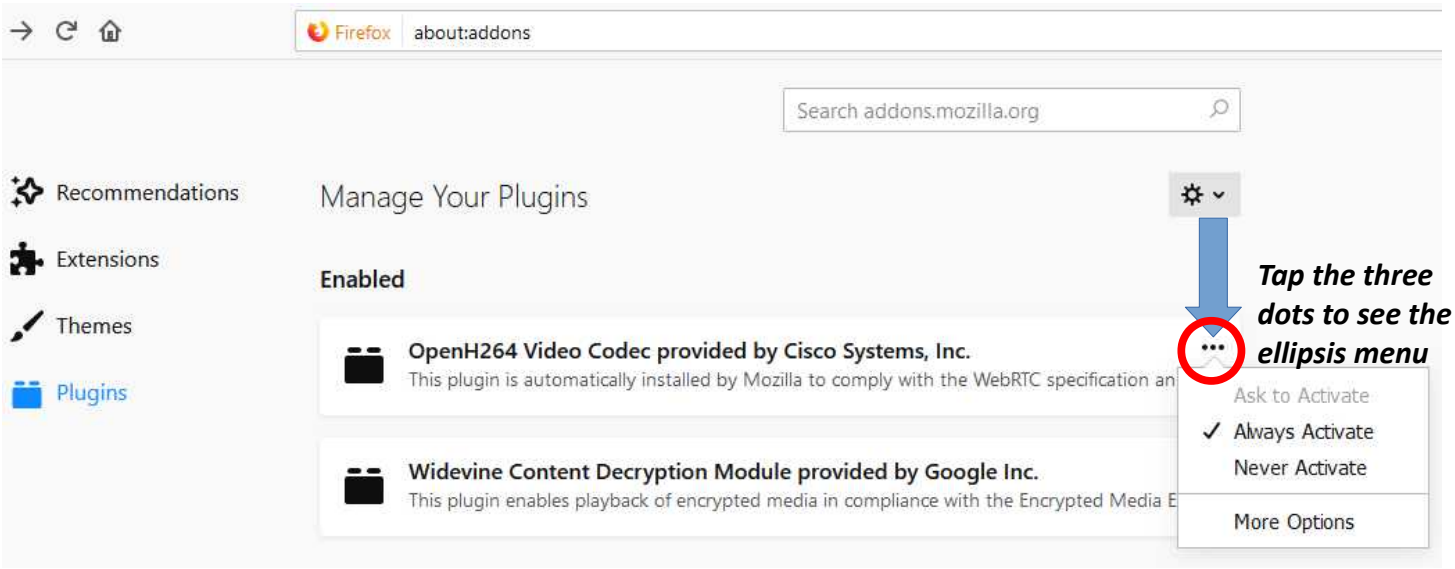

Illustration 6. Firefox Privacy & Security page with Plug-ins selected

There are four links in a vertical list in the left hand side of the page: Recommendations, Extensions, Themes, and Plug-Ins.

When I opened the page, **Plug-Ins** was selected, possibly because that is the choice I had made when I previously used

the about:addons page. When you access the page for the first time, Extensions may be selected.

This Plug-ins page reports I have two plug-ins installed and available for use. These no doubt were downloaded when I used Firefox to visit various Web sites. In particular, it is possible that the H.264 plug-in was installed when I visited CNN.com, since that site is chock-full of CNN videos these days. It is not surprising that Firefox does not recommend any plug-ins, since Firefox's policy is to get rid of the NPAPI itself and the plug-ins that caused such problems in Firefox.

The three dots to the right of each plug-in headline, known as an ellipsis, provide a way to disable each plug-in. Simply click on the ellipsis, and a dropdown menu appears, including four menu choices, as shown above. One of those choices effecitvely prevents use of the plug-in.

As shown above, I saw two plug-ins listed, both relating to media content. The OpenH264 Codec is from Cisco Systems, and plays various videos in the browser window. The Widevine Content Decryption module is from Google and is used to decrypt encrypted video. The encryption and decryption of video files is a way of ensuring that altered deep fake video is not associated with the good name of say CNN.com or Amazon Prime or Netflix.

On my laptop, I found the same two Firefox plug-in and one other: Adobe Flash. That one is also associated with media playback in the browser window.

I believe my antivirus software would tell me of any threat associated with these plug-ins, and I have not seen any threat report so far. If I found an unfamilair plug-in from an unknown company, then I would disable it immediately by choosing **Never Activate** in the ellipsis menu.

While reviewing the contents of directories on my hard drive that contain plug-ins, I found that each plug-in exists on the computer hard drive as a type of library file. For Windows computers, these are Dynamic Link Libraries (DLLs), each have the extension .dll at the end of the file name.

Here is a very important concern about libraries: they contain software that can accomplish literally anything possible using your computer. Some of those possible uses are, to put it mildly, not always in your best interests. Encrypt the hard drive and demand ransom? Of course. Erase the hard drive? No problem. Copy Your Contacts list and send it to who knows where? Sure. Capture all the credit card numbers you have typed into retailer web sites? Capture all of the IDs and passwords you type? You get the idea.

For this reason, I recommend a Firefox setting that forces Firefox to ask your permission when any web site attempts to install any extension or plug-in. As it happens, my antivirus software also informs me whenver such things get installed, but that notice shows up after installation happens. I prefer to have the choice beforehand.

This setting is on the same Privacy & Security page that I mentioned above. Scroll down to the Permissions heading. Under that heading, check Warn you when websites try to install add-ons. I believe the setting is in fact a Firefox default, so you are likely to find that it is already turned on. If not, then you can turn it on.

OK,now we return to the about:addons page.

Then I clicked **Themes.**

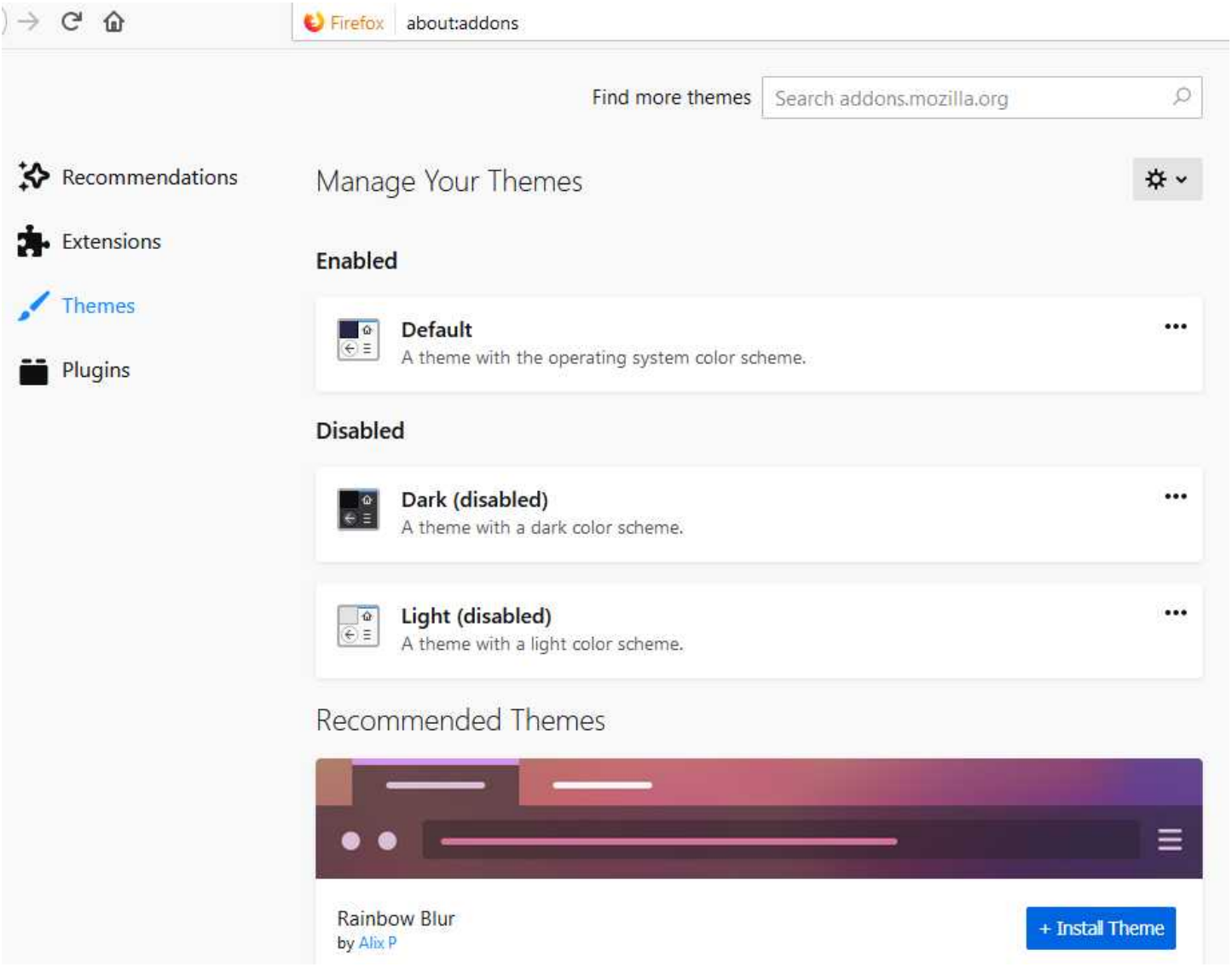

Illustration 7. Firefox about:addons page with Themes selected

This page reports I have one Theme in use, the one called Default, and two others installed. These appear to be delivered with Firefox itself, and I believe they are not harmful.

Then I clicked **Extensions**.

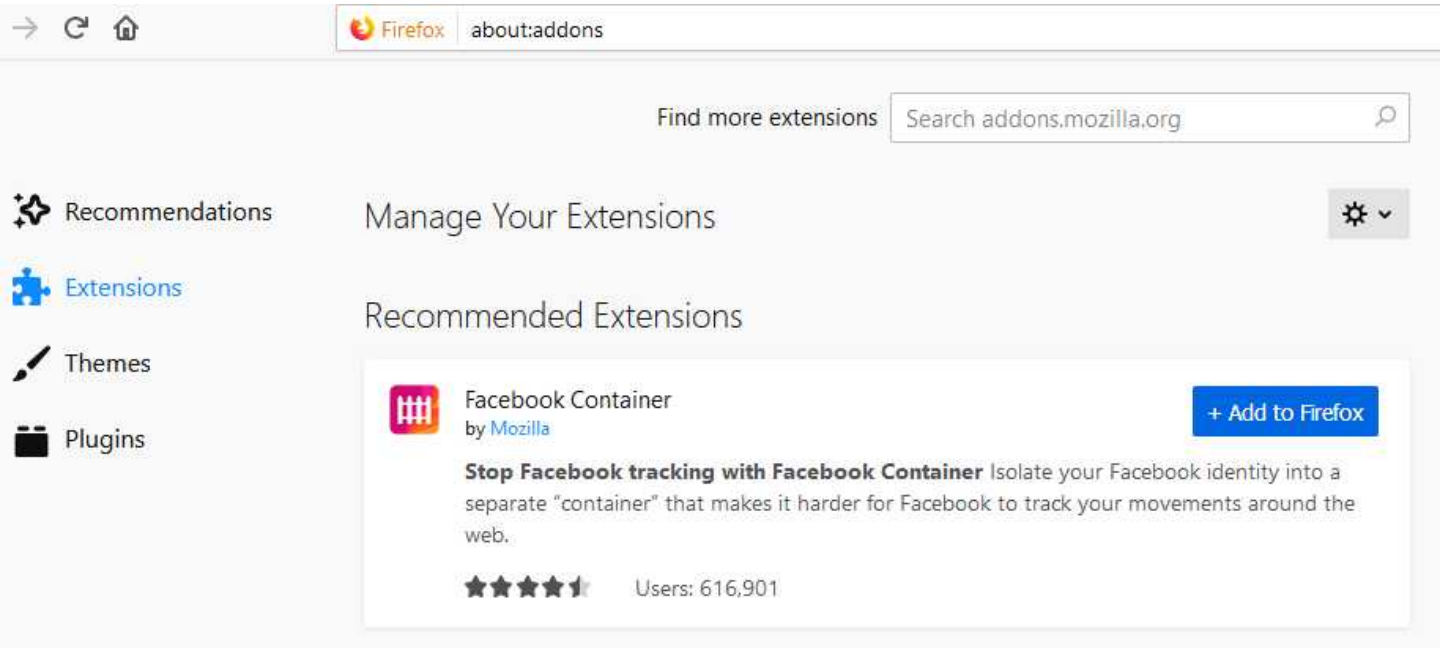

Illustration 8. Firefox Privacy & Security page with Extension selected

If you see the Manage Your Extensions heading with only the Recommended Extensions listed below it, which is the same status shown above, then you have **no extensions installed**. That is probably a good situation, since you have none to investigate and possible disable.

I think most extensions are Java code. Partly to see what happens when an extension ***is*** installed, I installed one of the recommended extensions called Privacy Badger, produced by the Electronic Frontier Foundation. It is an interesting extension that uses crowdsourcing to identify and eliminate even the nastiest cookies. So, if someone else who has installed Privacy Badger encounters a newly developed tracking cookie, Privacy Badger on your Firefox will be informed of the details and be prepared to block that cookie.

Here is how my Extensions list appeared after I installed that one Extension:

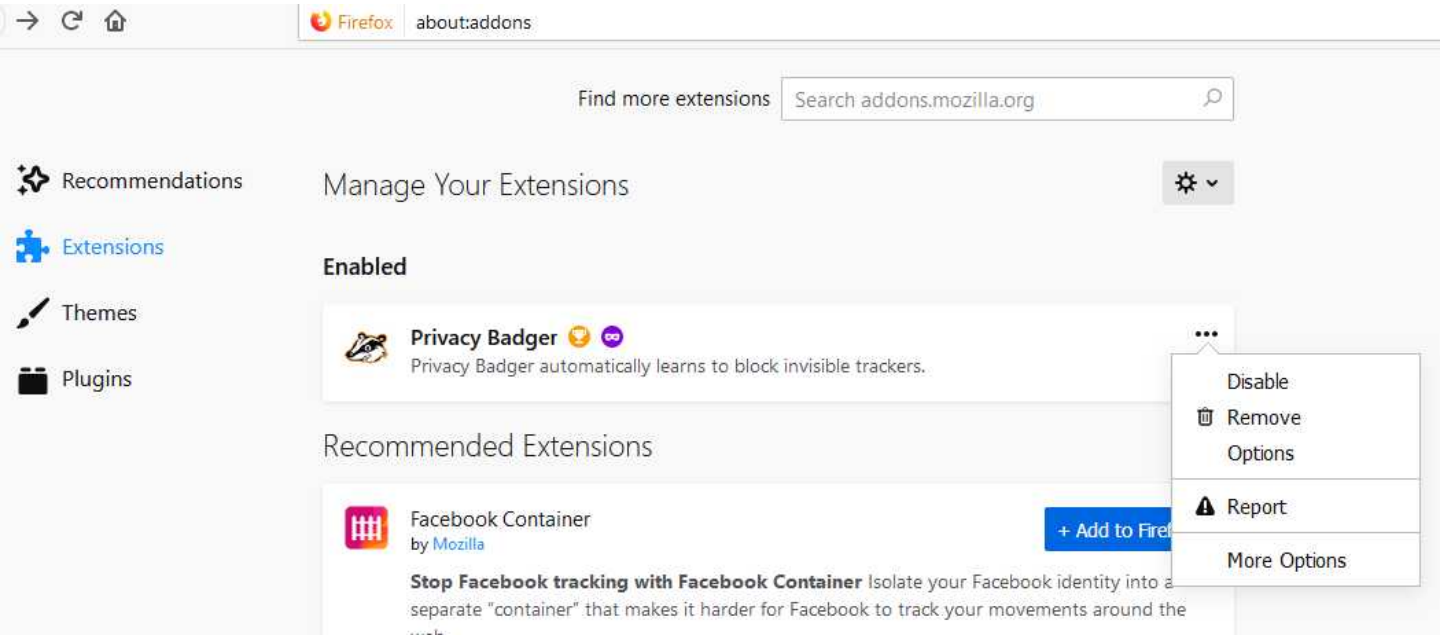

Illustration 9. Firefox about:addons page with one Extension installed

Obviously, tracking is performed by Facebook, as you can see from the description of the Facebook Container extension. Tracking is now arguably an epidemic.

When an extension is installed, an ellipsis menu is available. Click on the ellipsis and, as shown above, you will see a dropdown menu appear with options to disable and even remove the extension.

MANUAL ELIMINATION OF PLUG-INS

I found the following documentation section describing manual elimination of plug-ins. Using this elimination method, the DLL files are not literally removed, but their names are changed. When the name is changed, the browser or any web site or cookie in the browser cannot find and use the DLL file. Firefox does say most plug-ins are delivered with uninstallers, but nasty plug-ins certainly won't honor that recommendation, so these instructions are the one and only guaranteed universal uninstallation method.

Manually uninstalling a plugin

If you can't use an uninstaller program to remove a plugin, you can remove it manually:

Type about:plugins into the address bar and press Enter to display the About Plugins page.

Each entry in the About Plugins page will have "File:" and "Path:", showing the name and location of the plugin file. Use Windows Explorer to navigate to the folder shown for the plugin you want to remove.

Rename the file to add an X in front of the filename (for instance, npswf32 becomes Xnpswf32).

The plugin will be removed.

<end of documentation shard>

As mentioned above, I found two plug-ins on my recently purchased Windows desktop computer. Both I thought were not especially harmful. Here is the about:plugins page on that computer as of July 21, 2019.

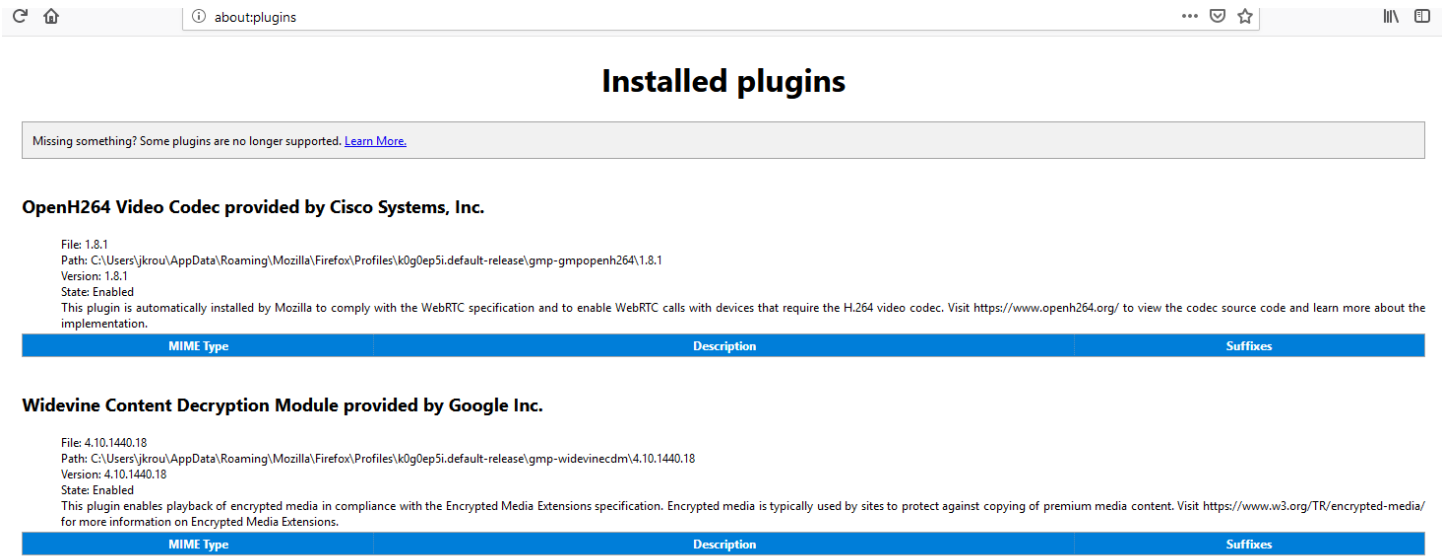

Illustration 10. Firefox about:plugins page showing directory path to find each plug-in

Uisng those directory path strings, I looked at the files involved using File Explorer (a.k.a Windows Explorer). That is how I found out the files were Dynamic Link Libraries.

It happens that the widevinecdm.dll file is updated fairly frequently by Google. So I see notifications maybe once a month or so indicating that the file is being installed.

That particular plug-in is published by Google as a way to avoid using Flash. It also ensures that the videos played by the DLL are not stored on your comptuer in a way that enables you to copy or alter the videos. There is a sort of ownership protection issue involved: none of the video owners want anyone to alter their video and suggest or imply that the altered video came from the owner.

This false attribution of altered videos is not in any sense a hypothetical concern. You may have read recently about an altered video that appears to show Speaker of the House Nancy Pelosi slurring words as though she were intoxicated. That video was an example of an altered video, carefully manipulated by computer to create that appearance. The altered video was entirely untruthful, mendacious, a lie.

Alas, like the software utilized to design nuclear bombs, the software used to alter videos is no longer very expensive. Economics is no longer a barrier. So it is important to prevent illicit alteration of legit videos.

HOW TO DELETE COOKIES ALREADY INSTALLED ON YOUR FIREFOX BROWSER

After reviewing this article, it occurred to me that it may be useful simply to delete all the cookies installed in my Firefox browser. That is not very difficult, as it happens.

1. Option the Firefox Options page (see Illustrations 1 and 2 above).

2. Scroll down to the heading Cookies and Site Data, as shown below.

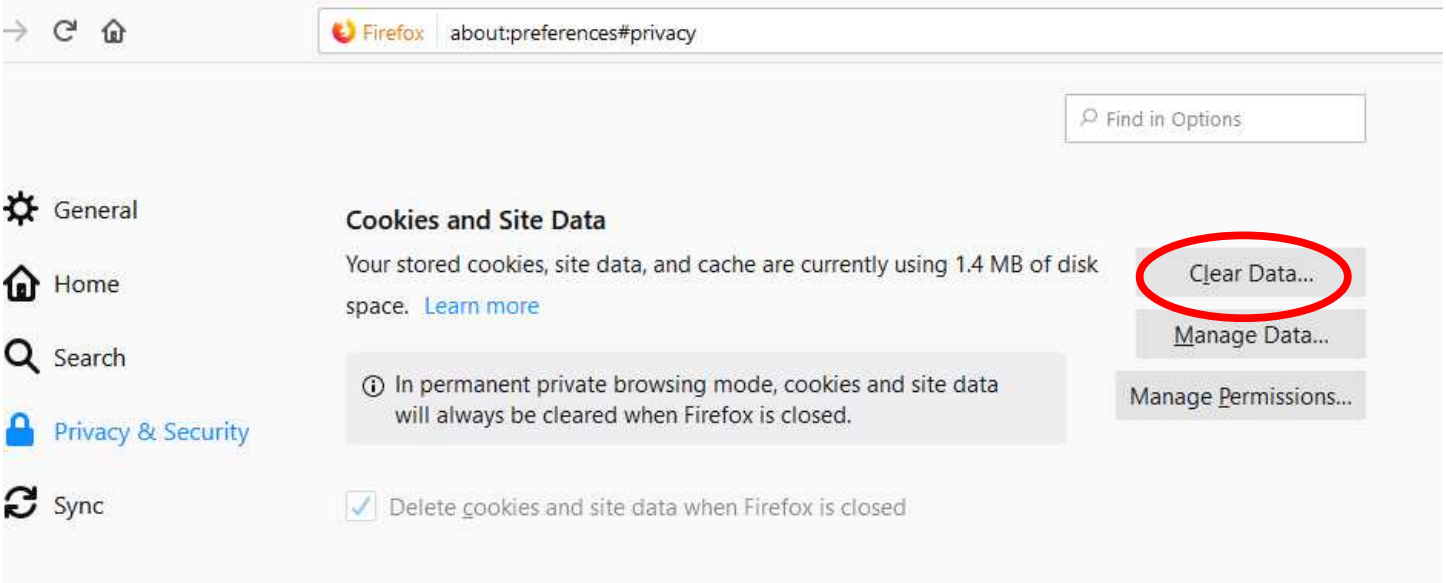

Illustration 11. Firefox Options page scrolled to Cookies and Site Data heading

You can see that I had 1.4 megabytes of cookies, site data, and cache data on my disk at the time I captured this screen image.

2. Click on the **Clear Data** button, which is circled above. Firefox pops up a window, as shown below. I call this the Consequences window.

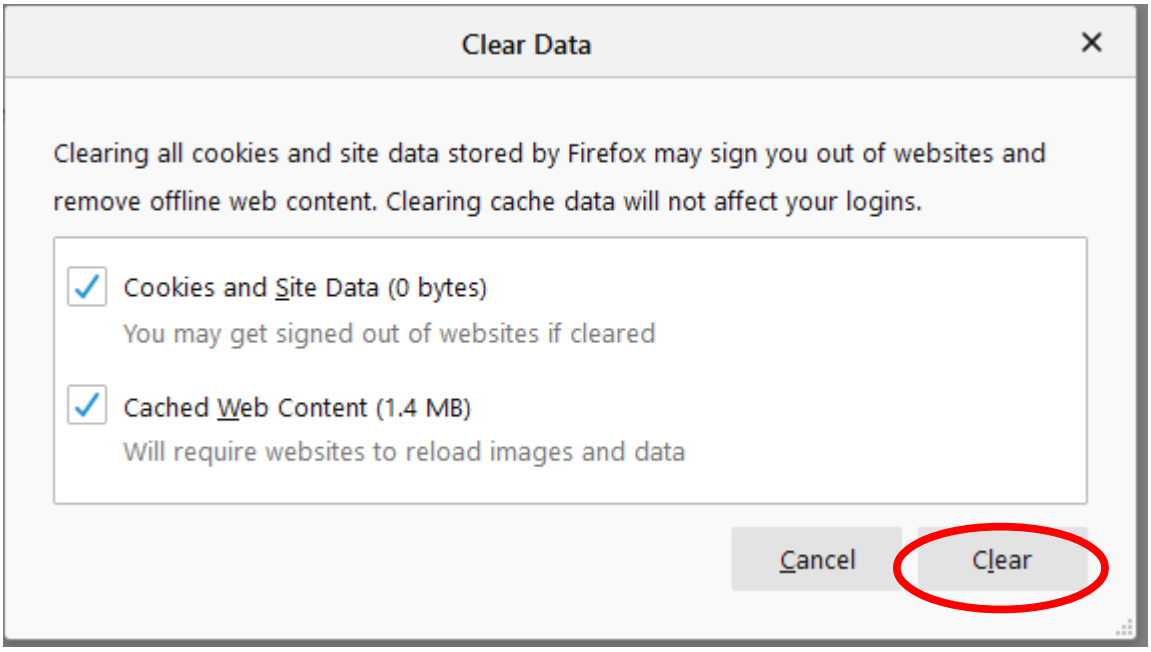

Illustration 12. The Firefox Clear Data Consequences window

This box actually told me a bit more. I had zero cookies, but I had 1.4 megabytes of cached web contents. This is stored by Firefox in the event that you return to a site you have visited recently, for rapid page display assuming the page has not changed. That is probably not a good assumption in most web sites I visit, so I am happy to remove the cached Web content.

3. Click on the Clear button, which is circled in the illustration above.

Firefox pops up one more requestor window, emphasizing that you are clearing out valuable info.

Click on the Clear Now button.

AND FINALLY

That's all I was able to learn in several evenings. I won't claim this is the last word on the subject, but rather a work in progress. Because the world often creates new ways to invade your computer, and then the browser publisher figures out new ways to stop it, or slow it down. The battle never ends.

I hope these instructions are easy to understand (I have some doubts about that but I tried my best) and easy to use.