Security Now! #995 - 10-08-24

uBlock Origin & Manifest V3

This week on Security Now!

Meta was not bothering to hash passwords? PayPal to begin selling its user's purchase histories. 2021's record for maximum DDoS size has been broken. It's national cybersecurity month. When was the last time you updated your router's firmware? North Korean hackers are successfully posing as domestic IT workers. Why would a security-related podcast ever talk about Vitamin D? What's another way the recent Linux CUPS vulnerability might be weaponized? What's the secure consumer WiFi router of choice today? And what should be done to further secure it after purchase? Recent troubles with uBlock Origin's Lite edition shine a light on Chrome's coming content-blocking add-on restrictions. What's going on and what can be done?

Modern product packaging can be a challenge

Security News

Facebook's parent Meta not hashing passwords

ArsTechnica carried the news that officials in Ireland fined Meta $101 million for storing hundreds of millions of user passwords in plaintext rather than hashing them for breach and employee abuse protection.

ArsTechnica first reported this conduct five years ago, back in 2019, under their headline *"Facebook apps logged users' passwords in plaintext, because why not"* with the subhead *"Unencrypted user credentials stored on Facebook internal servers as far back as 2012."* We talked about this at the time, but as a reminder, back in 2019, Ars wrote:

> *Facebook has mined a lot of data about its users over the years—relationships, political leanings, and even phone call logs. And now it appears Facebook may have inadvertently extracted another bit of critical information: users' login credentials, stored unencrypted on Facebook's servers and accessible to Facebook employees.*
>
> *Brian Krebs reports that hundreds of millions of Facebook users had their credentials logged in plain text by various applications written by Facebook employees. Those credentials were searched by about 2,000 Facebook engineers and developers more than 9 million times, according to a senior Facebook employee who spoke to Krebs; the employee asked to remain anonymous because they did not have permission to speak to the press on the matter.*

I recall this event because those numbers were so outrageous. Now Ars is reporting five years later that Facebook has spent these past five years "investigating" this. A heading in Ars reporting reads: "Meta investigated for five years". But it seems to me that the term "investigated" should be put in air quotes because it's difficult to see how an "investigation" of non-hashing could possibly require five years. If anything, the trail would have only grown more stale year after year as people who knew what happened became less accessible and more forgetful. So this feels a lot more like Facebook dragging their feet internally and not wanting to produce a final result of their investigation. But in any event, now Ars reports Graham Doyle, Ireland's deputy commissioner of Data Protection saying:

"It is widely accepted that user passwords should not be stored in plaintext, considering the risks of abuse that arise from persons accessing such data. It must be borne in mind that the passwords, the subject of consideration in this case, are particularly sensitive, as they would enable access to users' social media accounts."

So Ireland has been investigating the incident since Meta disclosed it and their Commission of Data Protection, which is the lead European Union regulator for most US Internet services, finally imposed a fine of $101 million (91 million euros) this week. So we can add that to the pile of fines that Facebook has incurred since the EU has fined Meta more than $2.23 billion (2 billion euros) for violations of the General Data Protection Regulation (GDPR), which went into effect in 2018. That amount includes last year's record $1.34 billion (1.2 billion euro) fine, which Meta is appealing.

I presume, though I haven't looked into it since it's not that interesting, that these fines are due to Facebook storing EU citizen data outside of the EU, likely in US-based data centers. What a mess.

A New, forthcoming PayPal default opts their users into merchant data sharing
Two weeks ago, PayPal posted a 60-day notice warning of a forthcoming change to their Privacy Statement which will become effective at the end of November on the 27th. The amendment says:

> *Notices / Issued: September 23, 2024*
> *Amendments to the PayPal Privacy Statement*
> *Effective November 27, 2024:*
>
> *We are updating our Privacy Statement to explain how, starting early Summer 2025, we will share information to help improve your shopping experience and make it more personalized for you. The key update to the Privacy Statement explains how we will share information with merchants to personalize your shopping experience and recommend our services to you. Personal information we disclose includes, for example, products, preferences, sizes, and styles we think you'll like. Information gathered about you after the effective date of our updated Privacy Statement, November 27, 2024, will be shared with participating stores where you shop, unless you live in California, North Dakota, or Vermont. For PayPal customers in California, North Dakota, or Vermont, we'll only share your information with those merchants if you tell us to do so. No matter where you live, you'll always be able to exercise your right to opt out of this data sharing by updating your preference settings in your account under "Data and Privacy."*
>
> *We are also making other updates to our Privacy Statement including some additional disclosures related to your right, depending on the jurisdiction in which you reside, to ask us for a list of the third parties to which we have disclosed personal information, and to provide other clarifying information.*

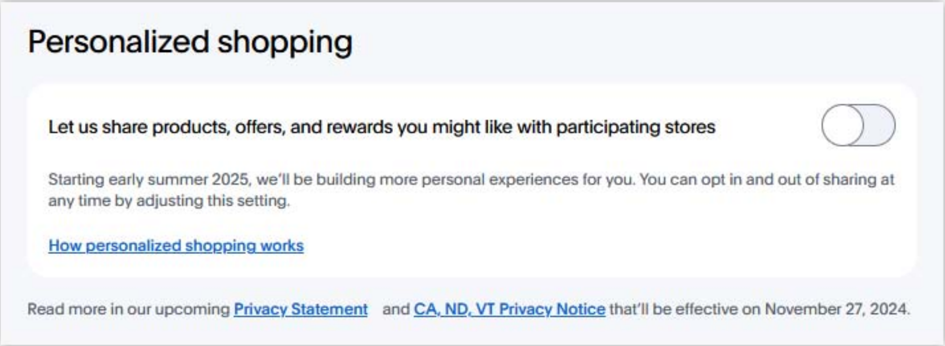
TechRadar carried the news of this, writing:

> *Another week, another online service silently changing its data collection and sharing practices by default. The good news is that you still have time to opt out before any of your information gets automatically given away without your consent.*
>
> *As per PayPal's policy updates page (issued on September 23 for US users), the service is set to exchange your data with third-party merchants "to help improve your shopping experience and make it more personalized for you." Starting in early Summer 2025, the new policy will not just come at the detriment of your privacy – even if you're using the best VPN apps – but PayPal will start gathering data as early as November 27, 2024.*
>
> *Users appear to be opted in by default, which may be an issue under some privacy regulations like GDPR. After coming across some US-based accounts complaining about this on Twitter, we decided to check if that was the case also for people in the UK. When we accessed privacy settings, the option was automatically toggled on.*
>
> *It's also important to bear in mind that the policy changes will not apply in the same ways across all jurisdictions and users. For instance, in the UK, the new data sharing is set to be enforced on October 10, 2024. A policy update dated July 8 clarifies that, for the UK market, "merchants are permitted to share customer personal information provided to them by PayPal with their service providers." We suggest checking your profile settings as soon as possible to reverse the change if you don't wish your data to be shared.*

I had to read part of that twice. In the UK, PayPal will be sharing its users' shopping histories with merchants and, in turn, those merchants will be permitted to share this personal information provided by PayPal with the customers' service providers. So UK-based ISPs, who are not PayPal merchants, will nevertheless obtain this information indirectly through the merchants who are. And note that all of these information-sharing activities are pretty much guaranteed to be for-pay arrangements. PayPal is unlikely to be sharing this valuable information With their merchants for free. Or if it is for free, then it represents an additional inducement for a merchant to offer PayPal payment. The pitch would be: *"Offer PayPal checkout and as an added benefit, we'll provide you with the detailed buying histories of the people who come to your website."*

The people who participate in discussions over in GRC's "thinktank" newsgroup know, because I was discussing the pros and cons there, that I had recently been considering reducing software purchase friction by adding PayPal checkout to GRC's e-commerce system. I decided not to, in the interest of remaining with the single universal credit card solution I've been using for the past 25 years. Learning of this, I'm certain I made the right decision since I would feel uncomfortable using a payment solution that defaults to profiling its users purchasing.

I use PayPal myself, but fortunately I'm in California. And while the "Nanny State" nature of California does occasionally annoy me and interfere with my choices, in this case I was glad to find that, indeed, that information sharing switch that almost everyone else will find is ON by default was OFF for me. For anyone who uses PayPal, after logging in, go to "Settings" which is a gear icon in the upper right if you're using a web browser. Under "Data & Privacy" you'll find the section "Manage shared info" and within that section you'll see "Personalized Shopping". If you select that option you'll be presented with some description and a big switch:



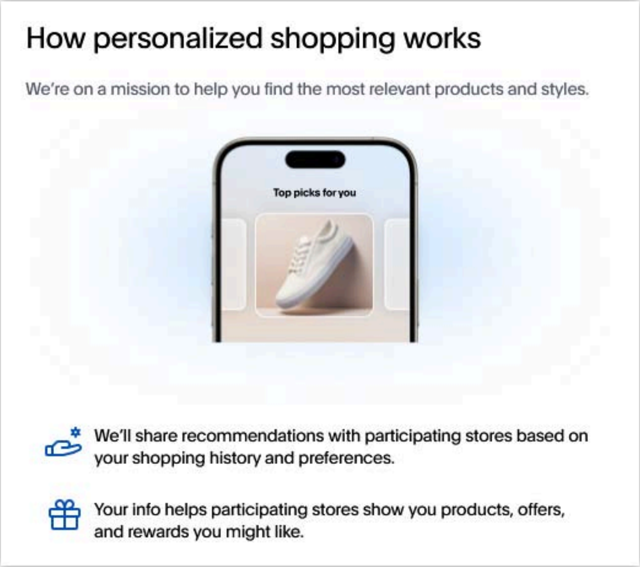
Personalized shopping

Let us share products, offers, and rewards you might like with participating stores

Starting early summer 2025, we'll be building more personal experiences for you. You can opt in and out of sharing at any time by adjusting this setting.

How personalized shopping works

Read more in our upcoming Privacy Statement and CA, ND, VT Privacy Notice that'll be effective on November 27, 2024.



How personalized shopping works

We're on a mission to help you find the most relevant products and styles.

We'll share recommendations with participating stores based on your shopping history and preferences.

Your info helps participating stores show you products, offers, and rewards you might like.

This is a new section and option that no PayPal user will have seen before. TechRadar explained that in the US, only residents of California, North Dakota and Vermont will find this turned off by default, with it being ON for everyone else, including those in the United Kingdom.

Underneath that big switch, I clicked a link with the text *"How personalized shopping works"*. That presents a pop-over explanation which says: *"We're on a mission to help you find the most relevant products and styles. We'll share recommendations with participating stores based on your shopping history and preferences. Your info helps participating stores show you products, offer, and rewards you might like."*

I know how this audience feels about Internet privacy since I've long enjoyed plenty of 2-way communication with our listeners, first through Twitter and then through eMail. So I wanted to be sure everyone using PayPal in the United Kingdom or in the US, who does not reside in California, North Dakota or Vermont, knew about PayPal's user purchase data sharing plans in time to preemptively say... "Gee, thanks, but no thanks".

Now, having said all that, I want to also acknowledge that both this past Sunday, two days ago, and also the Sunday before, PayPal very clearly notified me of these impending changes in a completely above board fashion. In the identical email I received on successive Sundays, they wrote: *"Our updated Privacy Statement outlines how we'll use info collected about you after November 27, 2024 to inform participating stores about what products, offers, and rewards you might like."* While we know that the Tyranny of the Default will work in their favor, and that defaulting to "opt-in" will see most people simply delete that email without pursuing it, thus leaving this new form of profiling enabled, they should be given due credit for working to clearly and even redundantly inform their users of this forthcoming change, and also for giving everyone 60 days advance notice before they first begin collecting this profiling data for release next summer.

DDoS breaks another record

Last Friday, Cloudflare disclosed that it had broken yet another record in fending off the largest DDoS attack ever seen on the Internet. Though the attack was brief, lasting only 65 seconds from start to finish, during those 65 seconds Cloudflare's infrastructure was hit by an attack that peaked at 3.8 terabits per second. Cloudflare is no stranger to DDoS attacks. Just in the last month it has fended off over one hundred hyper-volumetric Layer 3 & 4 DDoS attacks with many exceeding 2 billion packets per second.

These so-called hyper-volumetric Layer 3 & 4 DDoS attacks have been occurring since the start of September with their targets being multiple customers in the financial services, Internet, and telecommunication industries who use Cloudflare to remain on the air despite wire-melting attack levels. This recent record-breaking 3.8 terabits per second attack broke the previous record which had been set nearly three years before in November 2021. That attack peaked at 3.47 terabits per second and was attempting to blast an unnamed Asia-based Microsoft Azure customer off the Internet.

The attacks are using UDP packets aimed at a fixed port with the floods originating from Vietnam, Russia, Brazil, Spain, and the United States. Cloudflare said that the high bitrate attacks likely originate from a large botnet comprising infected ASUS home routers that have been exploited using a recently disclosed critical flaw – CVE-2024-3080 – having a CVSS of 9.8. According to statistics shared by Censys, a little over 157,000 ASUS router models were potentially affected by the vulnerability as of June 21, 2024. A majority of these devices are located in the U.S., Hong Kong, and China.

Speaking of these ASUS routers

I use an ASUS router for Wi-Fi service at my place with Lorrie, and even if that router were not safely perched behind a separate pfSense firewall appliance which connects it to the Internet, the last thing I would ever do would be to open a publicly accessible remote web admin portal. And I'm sure that listeners to this podcast have similarly protected themselves. But the Censys survey reveals that around 157,000 other ASUS owners have not been so circumspect.

Seeing this story I checked-in with my router. I don't have automatic updates enabled since my network has other security provisions. But it turned out that my router's firmware was a bit behind. I was running v3.0.0.4 and v3.0.0.6 was available. I have no trouble with the router, but updating always makes sense. And having layers of security is always a good thing.

Since this month of October is National Cybersecurity Awareness month, let me take this occasion to suggest that everyone listening check their router firmware to see whether there's an update available beyond what's running now. I'm glad I did.

Do you know who you're hiring?

We've recently been looking at the growing problem of spoofed identities by remote workers. The news this past week is that more than a dozen blockchain companies have inadvertently hired undercover North Korean IT workers. According to a CoinDesk investigation, this includes well-established blockchain projects such as Injective, ZeroLend, Fantom, SushiSwap, Yearn Finance, and Cosmos Hub. In every case, the workers passed checks using fake IDs and fake job histories. Aside from it being an obviously bad idea for any cryptocurrency company to allow an agent of a foreign government inside any sensitive organization, it's also completely against the law in the US and other countries that sanction North Korea.

Closing the Loop

Chris

Hi Steve, I am a longtime listener to Security Now, but last week as I was hiking in the White Mountains it occurred to me that there is one episode of this podcast that literally changed my life, and that was the Vitamin D episode. Ten years ago I would listen to podcasts while lying in bed suffering from debilitating back pain. My doctor had prescribed a big bottle of opioids, and I was desperate for an alternative, when I heard you and Leo mention Vitamin D and your past episode. I went back to the archive and listened to the Vitamin D episode, then went to my doctor and made him test me. My Vitamin D level was extremely low. I started taking 4,000 IU daily and over the course of a year I threw out the pain meds and started to feel much better. I would likely be bedridden and addicted to painkillers, rather than hiking in New Hampshire, had I not started taking Vitamin D. I think it's been a couple of years since I heard you mention Vitamin D on the podcast, so I want to urge you to remind people about that episode and your Vitamin D page in case there is anyone else out there facing a similar situation. Thank you, Chris

It was our audio-only podcast #209 recorded on August 13th, 2009. At the time, I had been spending a lot of time researching health and nutrition. I would take something – a vitamin or a mineral – and read one or more books about it, cover to cover. And that research has had a profound effect upon the lives of myself, my family and my friends. That research began exactly 20 years ago, shortly before I turned 50 and it turned me into a crazed consumer of dietary supplements. I have no way of knowing whether I would feel as fantastic as I do today if I hadn't been consuming a wide range of supplemental nutrition for the past 20 years. We'll never know. But I do know that there's still a lot more that I want to accomplish, so I'm going to keep doing what I've been doing since, if nothing else, it certainly doesn't appear to be hurting.

However, I know that for many people, consuming lots of supplements may not be practical for many reasons. Many people dislike taking pills; they can upset stomachs and they are an added cost over and above one's normal diet. For that reason, I've been extremely selective about what I've shared from my research. But I felt compelled to steal an early episode of Security Now! to explain what I had learned about Vitamin D. What you will find in that podcast is an explanation of the science and biochemistry of Vitamin D and the many reasons why it is so crucial to human health. The spring following that podcast I received many notes from our listeners who reported that for the first time in their lives they and their family, who were also taking a useful amount of Vitamin D had sailed through the winter without so much as a sniffle. And years later we saw an example of Vitamin D's powerful benefits for our immune systems during the world's struggle with COVID-19. Multiple studies revealed a strong correlation between vitamin D status and COVID outcome for those who had been infected.

So the reason I chose to talk about Vitamin D is that only micrograms of it are required. That means that a useful daily dose of four or five thousand IU is delivered in a tiny easy-to-swallow capsule of olive oil – or, as I like to refer to them "little drops of sunshine" – and vitamin D is also very inexpensive, with a year's supply available for around $15.

Everyone should keep in mind that I have no formal medical training of any kind. I'm a self-taught health hobbyist. So, thank you, Chris, for putting vitamin D back on the map for our many listeners who have joined us since we focused upon this valuable topic. I invite anyone who’s been made curious by this to listen to podcast number #209, for find edited-down audio at GRC under our main menu: Research / Health. Or just “Google” GRC Vitamin D and you’ll be rewarded with links.

Shane Overturf, IT Consultant

> *Steve, You've probably already seen this article by Akamai regarding the CUPS vulnerability, but in case you haven't, I thought it would interest you.*
> https://www.akamai.com/blog/security-research/october-cups-ddos-threat
> *While it's true that most people aren't going to be exposing port 631 to the Internet, and I can't think of a valid reason to expose it, it's apparent there are a fair number of those who do have it exposed. The Akamai article shows how trivial it is to leverage this vulnerability into a much more serious and widespread attack (something that you alluded to in the last podcast). So for the devs to dismiss it as "not so bad" seems to be a dangerous attitude. Looking forward to Security Now! “boldly go[ing] where no man has gone before” to 999 and beyond.*

I’m glad that Shane brought this to my attention. Last week I noted in passing that a handful of other security researchers had also examined the CUPS vulnerability. But I didn’t dig into them. Akamai’s findings are a bit chilling because they note that the presence of the cups-browse service listening on that port 631 allows it to be used in amplifying reflection attacks.

Giving their write-up the title “When CUPS Runneth Over: The Threat of DDoS” Akamai wrote:

> *Akamai researchers have confirmed a new attack vector using CUPS that could be leveraged to stage distributed denial-of-service (DDoS) attacks. Research shows that, to begin the attack, the attacking system only needs to send a single packet to a vulnerable and exposed CUPS service with internet connectivity. The Akamai Security Intelligence and Response Team (SIRT) found that more than 198,000 devices are vulnerable to this attack vector and are accessible on the public internet; roughly 34% of those could be used for DDoS abuse (58,000+). Of the 58,000+ vulnerable devices, hundreds exhibited an “infinite loop” of requests. The limited resources required to initiate a successful attack highlights the danger: It would take an attacker mere seconds to co-opt every vulnerable CUPS service currently exposed on the internet and cost the attacker less than a single US cent on modern hyperscale platforms.*
>
> *While reviewing the technical write-up about the vulnerabilities, we discovered that another attack vector was not discussed: DDoS. DDoS continues to be a viable attack vector used to harass and disrupt victims across the internet, from major industries and governments to small content creators, online shops, and gamers. Although the original analysis focused on the RCE – the Remote Code Execution – which could have a more severe outcome, DDoS amplification is also easily abused in this case.*
>
> *The problem arises when an attacker sends a crafted packet specifying the address of a target as a printer to be added. For each single packet sent, the vulnerable CUPS server will generate a larger and partially attacker-controlled IPP/HTTP request directed at the specified target. As a result, not only is the target affected, but the host of the CUPS server also becomes a victim, as the attack consumes its network bandwidth and CPU resources.*
>
> *We should note that many of these identified machines were running on very old versions of CUPS, such as version 1.3, which was initially released in 2007. It isn’t uncommon for some*

> *organizations to leave machines running on extremely outdated hardware and software, and it is unlikely that such devices will be updated anytime soon. This presents a prime opportunity for malicious threat actors: They can take advantage of the outdated hardware for DDoS amplification, or (given the RCE in this scenario) build botnets for many purposes, including DDoS.*

A listener who requested anonymity
I happened to notice that this person had added themselves to GRC's email system but had not subscribed to either the GRC or Security Now! Mailing list. Then, I saw her email in the security now mailbag and realized that she has registered her email specifically so that she could send this note. So how could I not share it? Besides, it's a terrific question which suggests a generally useful answer. So, this listener asked:

> *Hello Steve,*
>
> *I've been listening to your show for a few years, thanks to the recommendation of my former coworker. I am following more than I could at first and think I catch the general gist, but still miss significant bits of the technical know-how.*
>
> *Could you please recommend what is the most secure out-of-the-box residential router for non-technical folks, please? I want to replace my parents' router for multiple reasons. Primarily, since I can longer access the online admin portal to update the firmware, which is HTTP, and concerns about TP-Link backend. I've heard suggestions, such as use PFSense, but I've also heard that it would be easy to misconfigure something. I'm in a non-technical role, and I might be able to follow a youtube video potentially, but I'm concerned about missing configurations. Would greatly appreciate it if you or the community could please recommend a budget-friendly residential router that is secure by default without needing end user configuration. Thank you. (And I'd appreciate not having my name mentioned on the show, please.)*

I liked this listener's question because today's mainstream consumer routers are **all** going to be secure by default. And moreover, after enabling automatic firmware updates they ought to keep themselves secure in the event of anything significant happening. Disabling UPnP and WPS is a good idea, too. Consumers **primarily** get into trouble when they enable the additional extra fancy features that are being promoted to sell these routers today; things like remote WAN-side admin or any sort of Internet accessible media, file or other server. As we've seen over and over and over, there is no safe and secure way to do any of that. There **are** secure ways to accomplish those things, though they are more complex. They're more complex because more complexity is required to do those sorts of things securely.

Our listener's parents don't need any of that. They just need a nice generic SOHO NAT router. I'm partial to ASUS and I don't think I'd look any further since something in ASUS's line would likely be a good match. They start at $66 dollars US, so definitely budget-friendly and they support disabling WPS and UPnP, isolated WiFi guest networks for guests and IoT devices. A listener of ours, Michael Horowitz maintains a terrific website at: https://routersecurity.org.
I recommend Michael's site without reservation for any additional router security research.

uBlock Origin & Manifest V3

It’s been several years since we’ve talked about the web browser content blocker that’s heavily favored by the Internet’s more tech savvy users. It’s this podcast’s favored content blocker. I have it installed everywhere possible and I’ve often commented when I see unfiltered websites, that I cannot imagine not having uBlock Origin filtering the mess that the Internet has become.

Unfortunately, web browsers are gradually tightening the screws on the freedoms that add-on extensions such as uBlock Origin have traditionally enjoyed and upon which they depend. The Chrome browser’s eventual shift from Manifest v2 to Manifest v3 promises to make life much more difficult – if not impossible – for add-ons like uBlock Origin to continue to provide the features we’ve grown to depend upon.

And there’s been some recent turbulence involving uBlock Origin, Mozilla and uBlock Origin’s cantankerous creator, developer and maintainer Raymond Hill who goes by the moniker “Gorhill”. We’ll get to the recent trouble between Mozilla and Gorhill in a minute where some 7 million installations of uBlock Origin are installed. Let’s first look at what’s going on with uBlock Origin and the future of the Chrome browser which has around 37 million installations.

The Neowin site recently published a nice summary with background titled *“uBlock Origin developer recommends switching to uBlock Lite as Chrome flags the extension”* They wrote:

> *Google recently released Chrome 127 in the Stable Channel, and the update caused some commotion among certain customers. Those using the uBlock Origin extension, one of the most popular and well-received ad blockers, noticed that the browser now flags the extension with the following message:*
>
> > *uBlock Origin: This extension may soon no longer be supported.*
> > *Remove or replace it with similar extensions from the Chrome Web Store.*
>
> *Makers of the uBlock Origin extension [meaning Gorhill] published an article on GitHub that explained why Google Chrome claims uBlock Origin “may soon no longer be supported.” Long story short, the message appears due to Google's plans to deprecate Manifest V2-based extensions in favor of Manifest V3. For those unfamiliar, Manifest is a set of rules that defines how extensions integrate into browsers and interact with web pages. Migration from Manifest V2 to V3 has been long in the making. It faced tremendous criticism from users and developers, forcing Google to delay its plans and implement various changes to address complaints.*
>
> *Despite multiple changes, Manifest V3 still imposes significant limitations on browser extensions, especially content blockers.* ***There is no Manifest V3-based uBlock Origin****, so the developer recommends uBlock Origin Lite, a “pared-down” Manifest V3-compliant version of the extension. Like uBlock Origin, uBlock Lite prioritizes reliability and efficiency, but it has to compromise some features that are now impossible with Manifest V3. There is a dedicated web page that describes the difference between uBO and uBO Lite.*
>
> *Since the switch to Manifest V3 cripples the extension quite a lot, the developer does not plan to implement an automatic upgrade in the Chrome Web Store. Therefore, users can either stick to it until the bitter end or look for Manifest V3-compliant alternatives, such as uBO Lite or others.*

On this point, Gorhill wrote:

> *Manifest v2 uBO will not be automatically replaced by Manifest v3 uBOL. uBOL is too different from uBO for it to silently replace uBO -- you will have to explicitly make a choice as to which extension should replace uBO according to your own prerogatives. Ultimately whether uBOL is an acceptable alternative to uBO is up to you, it's not a choice that will be made for you.*

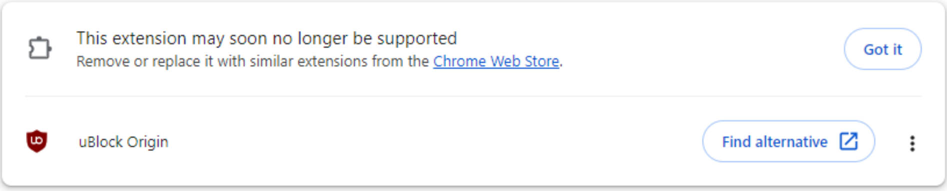
And Neowin's coverage concludes with:

> *According to the most recent announcement, Google plans to finish the migration to Manifest V3 by the end of 2024. However, enterprise customers will have the ability to continue using Manifest V2 extensions for six additional months. Interestingly, Mozilla, the only mainstream browser maker that does not use Chromium* [I suppose if you ignore all Apple browsers]*, does not plan to ditch Manifest V2 extensions. Therefore, uBlock Origin will continue working in Firefox and other browsers that do not deprecate V2 extensions.*

Although Chrome is reported to already be deprecating Manifest V2 in favor of V3, I just checked and my Chrome is running the full uBlock Origin without complaint. But that might not last long since Google has said that it will be finished with this migration three months from now. In their Manifest V2 support timeline document, Google wrote:

> *June 3 2024: the Manifest V2 phase-out begins.*
>
> *Starting on June 3 on the Chrome Beta, Dev and Canary channels, if users still have Manifest V2 extensions installed, some will start to see a warning banner when visiting their extension management page - chrome://extensions - informing them that some (Manifest V2) extensions they have installed will soon no longer be supported. At the same time, extensions with the Featured badge that are still using Manifest V2 will lose their badge.*

So I fired up Chrome and went over to chrome://extensions and sure enough:



This extension may soon no longer be supported

Remove or replace it with similar extensions from the Chrome Web Store.

uBlock Origin

"This extension may soon no longer be supported." – uBlock Origin. Hmm. Google continued:

> *This will be followed gradually in the coming months by the disabling of those extensions. Users will be directed to the Chrome Web Store, where they will be recommended Manifest V3 alternatives for their disabled extension. For a short time after the extensions are disabled, users will still be able to turn their Manifest V2 extensions back on, but over time, this toggle will go away as well.*
>
> *Like any big launches, all these changes will begin in pre-stable channel builds of Chrome first – Chrome Beta, Dev, and Canary. The changes will be rolled out over the coming months to Chrome Stable, with the goal of completing the transition by the beginning of next year.*

And this timeline document ended with the statement:

> *Enterprises using the ExtensionManifestV2Availability policy will be exempt from any browser changes until June 2025.*

That’s interesting. What’s this *“ExtensionManifestV2Availability”* policy and where can I get one?

So I tracked that down. It applies to Windows, Mac and Linux builds of Chrome. Google’s description for the policy is: “Control if Manifest v2 extensions can be used by browser.” ... which sounds like exactly what we want. The details are:

> *Manifest v2 extensions support will be deprecated and all extensions need to be migrated to v3 in the future. More information and timeline of the migration can be found at https://developer.chrome.com/docs/extensions/mv3/mv2-sunset/.*
>
> *If the policy is set to Default (0) or not set, v2 extensions loading are decided by browser, following the timeline above. If the policy is set to Disable (1), v2 extensions installation are blocked, existing ones are disabled. The option is going to be treated the same as if the policy is not set after v2 support is turned off by default. If the policy is set to Enable (2), v2 extensions are allowed. The option is going to be treated the same as if the policy is not set before v2 support is turned off by default. Extensions availability are still controlled by other policies:*
>
> *0 = Default browser behavior*
> *1 = Manifest v2 is disabled*
> *2 = Manifest v2 is enabled*
> *3 = Manifest v2 is enabled for forced extensions only*

As a reminder, Chrome’s “forced extensions” are installed by enterprise policy. They are installed silently without user interaction, bypassing the user interaction installation process and user’s are unable to remove extensions that are force-installed. Setting this V2 Extensions policy to ‘3’ causes the use of Manifest V2 to only apply to forced extensions whereas setting the policy to ‘2’ causes the Manifest V2 extension to apply to all extensions. So that’s the setting we want.

Doing this will buy savvy Chrome users an additional six months – through June 2025 – access to any of their current extensions that may not be V3 compatible (not only uBlock Origin).

For Windows systems, this policy can be applied by adding a 32-bit DWORD value to the Windows registry. This can either be done by hand or by executing a .REG registry file. To make this as easy and foolproof as possible for our listeners, I’ve created a GRC shortcut which will allow you to instantly obtain a three-line registry file from GRC:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome]
"ExtensionManifestV2Availability"=dword:00000002
```

The shortcut is https://grc.sc/v2. That will offer your browser a file to download named “V2Extension.reg”. You can open it in a text editor to verify its contents or to get the exact spelling for manual entry. Either way you can double click on the file to execute it directly. Since the fail has come to you from the Internet it will carry the “Mark of the Web” (MOTW) which will cause Windows to scrutinize it further. Since .REG files are just text files, they cannot be digitally signed. So I was unable to give it GRC's blessing. So Windows will inform you that the source of the file cannot be verified and ask if you're sure. Once you say "yeah, it's okay, I know the guy" you'll get another pop-up, this time from the Registry Editor explaining that running .REG files can mess things up and that you should only proceed if you know and trust the source of the file and are you sure you want to continue. If you click "Yes" your system will have added a policy to Chrome instructing it to continue allowing Manifest V2 extensions to run without harassment until next summer.

A cool thing you can do to verify and see this new policy in Chrome is to put chrome://policy into the URL. This will take you to Chrome's policies page where the new policy should be listed near the top. If it's not, there's a "Reload Policies" button at the top-left that will cause Chrome to check for and display any recent changes.

So, making this change buys Chrome users an additional 6 months of access to the full uBlock Origin and any other beloved Chrome extensions that require Manifest V2. In the case of uBlock Origin, no matter what, if you remain with Chrome, come June of 2025 you'll need to switch over to uBlock Origin Lite. This brings us to the question: What's the difference between the two?

Let me pause here for a moment to comment on Manifest V2 vs V3. Overall, this migration to Manifest V3 is a good thing for browser performance and security. One way to look at the difference is that whereas V2 causes our browsers to hand over control to each extension and effectively say "have at it, do whatever you want", the changes coming in V3 cause our browsers to ask each extension "tell me what you would like to have done and I'll do it for you." It should be obvious which of these two strategies provides the user with greater security and the browser with more control and oversight over what its extensions are intending to do. But it's also clear why and how this does, in return, somewhat cramp any extension's style. Extensions no longer have essentially free reign over the user's browser. As Gorhill expresses the difference, MV3 requires extensions to be "declarative" where the browser reads and executes the extension's declarations on its behalf.

So this brings us back to the question: What features does V2-compatible uBlock Origin sacrifice in the transition to V3-compatible uBlock Origin Lite? The uBOL (uBlock Origin Lite) Github repository has an FAQ page which answers this question in detail, but Wikipedia offers a more accessible summary, writing:

> *In 2023, Google made changes known as "Manifest V3" to the WebRequest API used by ad blocking and privacy extensions to block and modify network connections. Following Google's implementation of Manifest V3 and the end of support for V2, uBlock Origin's effectiveness is drastically reduced in Google Chrome and other Chromium-based browsers.* [Note that while this sounds, and is, bad, this is not any failing in uBlock Origin. It is true universally of all content control add-ons under MV3. This is why Google has been met with significant pushback and why the EFF is apoplectic. Wikipedia elaborates:]
>
> *As a result, uBlock Origin Lite was created and designed to comply with the Manifest V3 (MV3) extension framework. uBO Lite differs significantly from uBO in several key aspects, primarily due to the constraints and design goals associated with MV3. Specifically, it lacks filter list updates outside of extension updates, and has no custom filters, strict-blocked pages, per-site switches, or dynamic filtering.* ***Non-Chromium browsers such as Firefox*** *are unaffected. Google has been criticized for implementing some of these features due to its dominance in the online advertising market.*

https://github.com/uBlockOrigin/uBOL-home/wiki/Frequently-asked-questions-(FAQ)

Gorhill's FAQ page for uBO Lite asks and answers this question:

> *Q: If I install uBOL, will I see a difference from uBO?*
>
> *A: Maybe. Maybe not. It depends on:*
>
> - *Websites you visit*
> - *How you configured uBO*
> - *How you configured uBOL*
>
> *In short, only you can tell. It's very possible that the sites you visit do not require any of the filtering capabilities specific to uBO, in which case you won't see a difference. Also, mind that by default there is no cosmetic filtering or scriptlet injection in uBOL while these occur by default in uBO. In uBOL, you will have to raise the blocking mode to either Optimal or Complete to benefit from cosmetic filtering and scriptlet injection. Furthermore, uBOL requires the default mode to be Optimal or Complete for some advanced filtering capabilities to take effect, while they are enabled by default in uBO. In general, uBOL will be less effective at dealing with websites using anti-content blocking, or minimizing website breakage.*

So it doesn't sound like the end of the world for uBlock Origin Lite on Chrome which Chrome users will at least be able to delay until June of 2025.

So that's the story with Chrome and all of the closely related Chromium-based web browsers. The great news for the 7 million of us who are currently using the full uBlock Origin on Firefox is that Mozilla has officially stated that they have no plans to remove support for Manifest V2 from Firefox. Google is going to at least somewhat hamper Chrome's support for content-control add-ons whereas, at least as presently stated, Mozilla has no plans to do the same for Firefox.

However, uBlock Origin is so popular and well known that a recent kerfuffle between Mozilla and Gorhill regarding uBlock Origin Lite received a great deal of attention online.

Now, you may be thinking, did I say Mozilla and uBlock Origin LITE? And if so, why is there a Lite edition of uBlock Origin for Firefox when Mozilla has said that Firefox's support Manifest V2 is safe and will not be removed? The reason is that Gorhill just wanted to release the same add-on feature-set for Firefox that he had created for Chrome. He wanted to have a uBlock Origin Lite available for both major web browser platforms.

https://github.com/uBlockOrigin/uBOL-home/issues/197

A little over a month ago, Gorhill posted to Github that he had received two email from Mozilla Add-Ons and included the entire content of their email in his posting. Mozilla Add-Ons wrote:

> *Hello, Your Extension uBlock Origin Lite was manually reviewed by the Mozilla Add-ons team in an assessment performed on our own initiative of content that was submitted to Mozilla Add-ons. Our review found that your content violates the following Mozilla policy or policies:*
>
> ***1. Consent**, specifically Nonexistent: For add-ons that collect or transmit user data, the user must be informed and provided with a clear and easy way to control this data collection. The control mechanism must be shown at first-run of the add-on. The control should contain a*

> *choice accompanied by the data collection summary. Depending on the type of data being collected, the choice to send cannot be enabled by default. If data collection starts or changes in an add-on update, or the consent and control is introduced in an update, it must be shown to all new and upgrading users. For the exact requirements, refer to https://extensionworkshop.com/documentation/publish/add-on-policies/#data-disclosure-collection-and-management. For an example of how to provide a consent and control dialog, see https://extensionworkshop.com/documentation/develop/best-practices-for-collecting-user-data-consents/. Also, if your add-on is listed on addons.mozilla.org, the listing needs to include a privacy policy, and a summary of the data collection should be mentioned in the add-on description. -> web_accessible_resources/googlesyndication_adsbygoogle.js*

I'll interrupt to note that this is one of those "what have you been smoking and where can I get some?" things, since neither uBlock Origin nor uBlock Origin Lite has ever or would ever collect any sort of user data. If we know anything about Raymond Hill we know that.

But that's not all, point #2 was:

> ***2. Sources**, specifically Sources or instructions missing: Your add-on contains minified, concatenated or otherwise machine-generated code. You need to provide the original sources, together with instructions on how to generate the exact same code used in the add-on.*
>
> *Source code must be provided as an archive and uploaded using the source code upload field, which can be done during submission or on the version page in the developer hub. Instructions can be provided in a top-level README file inside the source code package or in the "Notes to Reviewers" field on the version page in the developer hub.*
>
> *-> web_accessible_resources/fingerprint2.js*
> *-> web_accessible_resources/google-analytics_analytics.js*
> *-> web_accessible_resources/google-analytics_ga.js*
> *-> web_accessible_resources/googletagservices_gpt.js.*
>
> *Affected versions: 1.0.23.8128, 1.0.23.8155, 2023.9.10.1131, 2023.9.19.787, 2023.9.28.935, 2023.10.3.896, 2023.10.12.904, 2023.10.21.720, 2023.11.4.95, 2023.11.11.1035, 2023.11.19.977, 2023.11.28.36, 2023.12.4.1333, 2023.12.16.1327, 2024.1.2.1038, 2024.1.14.912, 2024.1.21.1302, 2024.1.29.1338, 2024.2.14.104, 2024.2.25.1407, 2024.2.26.112, 2024.3.4.107, 2024.3.11.1438, 2024.3.21.842, 2024.3.30.1062, 2024.4.8.931, 2024.5.13.839, 2024.5.17.961, 2024.5.27.852, 2024.6.2.1013, 2024.6.10.805, 2024.6.17.766, 2024.6.26.1308, 2024.7.3.674, 2024.7.17.853, 2024.7.28.888, 2024.8.5.925, 2024.8.12.902, 2024.8.19.905, 2024.8.21.996, 2024.9.1.1266*
>
> *Based on that finding, those versions of your Extension have been disabled on https://addons.mozilla.org/addon/ublock-origin-lite/ and are no longer available for download from Mozilla Add-ons, anywhere in the world. Users who have previously installed those versions will be able to continue using them.*
>
> *You may upload a new version which addresses the policy violations.*
> *More information about Mozilla's add-on policies can be found at https://extensionworkshop.com/documentation/publish/add-on-policies/.*
>
> *Thank you for your attention.*

What was it we were observing last week about the thanklessness of the job of the open source free software developer?

As I mentioned there were two of these emails. The second listed exactly the same bogus add-on policy failures but only covered one version, the oldest version of all, published in August of 2023. That email gave its developer 14 days to cure before the extension would be pulled.

Gorhill's somewhat predictable reply in that github thread was:

> *Contrary to what these emails suggest, the source code files highlighted in the email:*
>
> - *Have nothing to do with data collection, there is no such thing anywhere in uBOL*
> - *There is no minified code in uBOL, and certainly none in the supposed faulty files*
> - *There is a privacy policy link in uBOL's add-on page: https://addons.mozilla.org/en-US/firefox/addon/ublock-origin-lite/privacy/*
>
> *I don't have the time or motivation to spend time on this nonsense, so I will let AMO do whatever they want with uBOL. I will probably publish a self-hosted version which auto-updates (like how dev build of uBO is self-hosted) when I find the time to arrange all that.*

"AMO" is short for "addons.mozilla.org". The following day, on September 5th, someone with the handle "Rob–W" posted:

> *@gorhill The review decision looks inaccurate to me. Could you reply to the email to let the original reviewers know that the assessment is inaccurate? What you wrote above in the comment is sufficient.*

Gorhill did not reply to that. But nearly two weeks later on September 18th, he posted:

> *Starting with uBOLite_2024.9.12.1004, the Firefox version of the extension will be self-hosted and can be installed from the release section. The extension will auto update when a newer version is available.*

And then on September 26th, Gorhill posted that he had changing his mind, writing:

> *The Firefox version of uBO Lite will cease to exist, I am dropping support because of the added burden of dealing with AMO's nonsensical and hostile review process. However trivial this may look to an outsider, it's a burden I don't want to take on — since the burden is on me, I make the decision whether I can take it on or not, it's not something up for discussion.*
>
> *The burden is that even as a self-hosted extension, it fails to pass review at submission time, which leads to having to wait an arbitrary amount of time — where time is an important factor when all the filtering rules must be packaged into the extension — and once I finally receive a notification that the review cleared, I have to manually download the extension's file, rename it, then upload it to GitHub, then manually patch the update_url to point to the new version. It took 5 days after I submitted version 2024.9.12.1004 to finally be notified that the version was approved for self-hosting. As of writing, version 2024.9.22.986 has still not been approved.*

> *However often I look at all this, every time I can only conclude the feedback from Mozilla Add-ons Team to have been nonsensical and hostile, and as a matter of principle I won't partake in this nonsensical and hostile review process.*
>
> *It takes only a few seconds to see how this is nonsensical -- keep in mind that this “was manually reviewed by the Mozilla Add-ons team”:*
>
> *“For add-ons that collect or transmit user data, the user must be informed and provided with a clear and easy way to control this data collection”*
>
> *Where is the "data collection" in this file?*
>
> *https://github.com/uBlockOrigin/uBOL-home/blob/uBOLite_2024.9.1.1266/firefox/web_accessible_resources/googlesyndication_adsbygoogle.js*
>
> *"Your add-on contains minified, concatenated or otherwise machine-generated code"*
>
> *Where is the "minification" in these files?*
>
> *https://github.com/uBlockOrigin/uBOL-home/blob/uBOLite_2024.9.1.1266/firefox/web_accessible_resources/fingerprint2.js*
>
> *https://github.com/uBlockOrigin/uBOL-home/blob/uBOLite_2024.9.1.1266/firefox/web_accessible_resources/google-analytics_analytics.js*
>
> *https://github.com/uBlockOrigin/uBOL-home/blob/uBOLite_2024.9.1.1266/firefox/web_accessible_resources/google-analytics_ga.js*
>
> *https://github.com/uBlockOrigin/uBOL-home/blob/uBOLite_2024.9.1.1266/firefox/web_accessible_resources/googletagservices_gpt.js*
>
> *"Also, if your add-on is listed on addons.mozilla.org, the listing needs to include a privacy policy, and a summary of the data collection should be mentioned in the add-on description."*
>
> *Right, it's always been there since the first version published on AMO more than a year ago*
> *https://github.com/user-attachments/assets/350bc17c-53e2-401a-91a0-2a321337c49e*
>
> *Incidentally, all the files reported as having issues are exactly the same files being used in uBO for years, and have been used in uBOL as well for over a year with no modification. Given this, it's worrisome what could happen to uBO in the future given it uses the same exact files.*
>
> *The steps taken by Mozilla Add-ons Team as a result of the (nonsensical) "issues" was to disable all versions of uBOL except for the oldest version, first published on AMO on August 2023. That oldest version is also reported as having the same "issues" and was set to be disabled by Mozilla Add-ons Team unless the "issues" were addressed ("Based on that finding, those versions of your Extension will be disabled in 14 day(s).").*

> *I disabled this version myself to prevent new users from ending up with a severely outdated version of the extension to avoid a subpar first experience of uBOL.*
>
> *So essentially, it was deemed that all versions of uBOL were having "issues", but instead of disabling all of them except the most recent one, they disabled all of them except the oldest one. This is hostile considering that whoever installed uBOL at that point would be installing a version of uBOL with severely outdated filter lists, along with an outdated codebase (many issues were fixed in the codebase since August 2023).*
>
> *I am unable to attribute good faith to both the nonsensical review feedback and the steps taken as a result of this nonsensical review feedback, and I am unable to take on the added burden of having to deal with nonsense.*
>
> *This is unfortunate because despite uBOL being more limited than uBO, there were people who preferred the Lite approach of uBOL, which was designed from the ground up to be an efficient suspendable extension, thus a good match for Firefox for Android.*
>
> *From this point on, there will no longer be a package published in the release section for Firefox, except for the latest one, uBOLite_2024.9.22.986, if and when it's approved.*

Raymond apparently received some additional non-sympathetic feedback about his decision to completely drop uBlock Origin Lite from Firefox since he final posting on October 1st, last Tuesday, was:

> *Looks like the sentence "however trivial this may look to an outsider, it's a burden I don't want to take on" is lost on many who want to have an opinion about all this.*
>
> *I dropped support for uMatrix years ago because it had become a burden I couldn't take on. This is such a case here, where the unwarranted de-listing of uBOL and the requirement of having to deal with this caused the support to maintain a Firefox version to cross the line into the "burden I can't take on" territory.*
>
> *Amount of burden to take on is a personal decision, not something to be decided by others.*

And just to add a bit of objectivity, since Gorhill has clearly taken a stand on this, here's a sympathetic comment I found, posted 6 days ago, over on Ycombinator:

> *I manage a medium-sized browser extension at work. We also offer(ed) it on Firefox. But I have spent the past year struggling to get back into Mozilla store after a manual review.*
>
> *As far as I can tell, there are maybe two reviewers that are based in Europe (Romania?). The turnaround time is long when I am in the US, and it has been rife with this same kind of "simple mistake" that takes 2 weeks to resolve:*
>
> - *"You need a privacy policy"–we already have one.*
> - *"You are using machine generated and minified code"–no you are looking at the built code, not the included source.*
> - *"We cannot reproduce your source"-that's because you didn't follow instructions and are in the wrong directory. Very frustrating.*

And there were a number of other similar comments. So it appears that Mozilla really does currently have a problem with this aspect of their bureaucracy and that Gorhill, someone who has – shall we say – an extremely low threshold of tolerance for any sort of incompetence that's impeding him, finally just decided that it wasn't worth his time or energy to fight a frustrating battle.

Okay. So we now have the full picture of exactly where uBlock Origin and its Lite edition stand.

Over on Chrome, Edge and other chromium-based web browsers, Google is in the process, right now, of lowering the boom on any extensions that presently require Manifest V2 which Chrome will be discontinuing. Anyone using Chrome can put chrome://extensions/ in Chrome's URL to see a summary of their currently installed extensions and without a policy override in place Chrome will show you which extensions are soon to be incompatible.

But nine months of additional Manifest V2 extension life can be had by enabling a policy to that effect. This is available across all desktop editions of Chrome and in Windows it can be obtained by adding a registry value. I've created a registry file named V2Extension.reg that anyone can obtain by going to grc.sc/v2. And based upon what Gorhill himself has stated, eventually being left with only the Lite edition of uBlock Origin should not be so bad. Because uBlock Origin Lite will not be able to proactively inject JavaScript code into sites to more fully tame them, the content on some sites may be less fully blocked, but it will still be far better to have what is arguably the best add-on content blocker than none.

And over on the Firefox side, Mozilla has stated that they do not intend to discontinue support for Manifest V2. This makes sense since it offers a true competitive benefit that Firefox will be alone in continuing to offer more powerful traditional add-ons. That feels like the reason savvy users choose Firefox in the first place.

And it appears to be fortunate that Mozilla will allow all of us to continue using the full Manifest V2 edition of uBlock Origin since its cantankerous developer has become quite annoyed with Mozilla's add-ons vetting team and has pulled his Manifest V3-compatible edition of uBlock Origin Lite from the running.

As I've long said, thanks to my use of uBlock Origin everywhere, my web pages look far more quiet and calm than those I see other people's browsers displaying. I always wonder how they can tolerate all that superfluous crap.

One topic this discussion has completely avoided, so far, is the large and significant question of the ethics surrounding editing received webpages to remove content – any content – that the website wishes to deliver and push on its visitors.

Tracking scripts are one thing; but the more controversial removal is that which produces revenue for the site. We know that today there are many websites that wholly depend upon the revenue from advertising to survive. And we need look no further than this podcast's own hosting network TWiT to see firsthand the effects of advertising revenue becoming less available than it once was.

So I'll finish today's discussion of the evolving technology of the browser add-on ecosystem by quoting the author of uBlock Origin. Raymond Hill, Gorhill, says the following on his Github page for his original full-spectrum content blocker, uBlock Origin. He writes:

> *uBlock Origin (uBO) is a CPU and memory-efficient wide-spectrum content blocker for Chromium and Firefox.*
>
> *It blocks ads, trackers, coin miners, popups, annoying anti-blockers, malware sites, etc., by default using EasyList, EasyPrivacy, Peter Lowe's Blocklist, Online Malicious URL Blocklist, and uBO filter lists. There are many other lists available to block even more. Hosts files are also supported. uBO uses the EasyList filter syntax and extends the syntax to work with custom rules and filters.*
>
> *You may easily unselect any preselected filter lists if you think uBO blocks too much. For reference, Adblock Plus installs with only EasyList, ABP filters, and Acceptable Ads enabled by default.*
>
> *It is important to note that using a blocker is NOT theft. Do not fall for this creepy idea. The ultimate logical consequence of blocking = theft is the criminalization of the inalienable right to privacy.*
>
> *Ads, "unintrusive" or not, are just the visible portion of the privacy-invading means entering your browser when you visit most sites. uBlock Origin's primary goal is to help users neutralize these privacy-invading methods in a way that welcomes those users who do not wish to use more technical means.*

We've spent a lot of time through the 19+ years of this podcast, as this industry has evolved, looking at this issue. If advertisements were visually static and non-intrusive. If they were not planting cookies in my browser and running code in an active attempt to fingerprint me for the purchase of tracking my movements and compiling a list of everywhere I go and everything I do, and if the websites hosting these obnoxious privacy-invaders were not actively complicit in this, then I would feel far more sympathetic to the need for websites to generate revenue by forcibly exposing me to things I do not want.

I do not believe that where we are today, in the year 2024, is where we will be ten years from now. If nothing else, we can see how the industry and government are struggling to come to agreement and compromise. I was disappointed that European regulators forced Google to abandon its significantly privacy-enforcing Privacy Sandbox technology. The fact that they were forced to give it up because it would have been so privacy-enforcing tells you all you need to know about the state of today's web technology.

Content control add-ons do not completely prevent tracking and profiling, but they mitigate it. And they do make the use of the web significantly more pleasant. One thing seems clear: If individual end users – the consumers of the ads and the targets of this tracking – do not push back within their means against this abuse of our attention and privacy, it's likely to take much longer for it to change.