Reality of FOSS projects...A conspiracy?

security, **foss**, **privacy**

TheMystic #1 September 23, 2021, 8:58am

KEY POINTS SUMMARIZED

1. FOSS is NOT necessarily anti-tracking, anti-analytics or anti-surveillance. FOSS isn't the solution if these things are what you want. FOSS 'may' free you from Google, but not necessarily from tracking.

2. FOSS platforms CAN have contributions (in the form of apps) from large corporations (like Google, Facebook, etc.) or intelligence agencies. App developers are often anonymous, and there is no assurance that they aren't working for a large corporation, intelligence agency or even a hacking group.

3. Apps may be masquerading as open source, when it is quite possible that only some of the libraries used in the app are open source, and there are hidden codes within the app that aren't actually open source.

4. There is no accountability/ audits for FOSS platforms. While they may make the platform available with good intent, there is immense scope for the same to be exploited.

5. If tracking and surveillance is something that you want to seriously avoid, there is ONLY ONE WAY: don't use gadgets and stay away from internet.

I guess most users in this forum are those who are looking for ANTI-TRACKING solutions. Some, including myself, are quite happy with Google products and services. The reason being the benefits outweigh the costs, and more importantly the fact that there is no clear understanding of what these costs are, or to put it differently, what risks are associated with so-called costs.

I believe, in the absence of convincing explanations, the risks are overstated and much of the paranoia is based on hypothetical situations/ circumstances. You can't have meaningful output without an input. A doctor can't prescribe correct medication if you don't tell him/ her the problems correctly. You have to let go of privacy if you want to solve a problem.

Having said that, I won't be surprised if Google, Apple, Microsoft, Qualcomm, Intel, AMD, etc. (who essentially cover the major OSes and Hardware all over the world, and used by more than 90% of the world population) are all companies run/ monitored by intelligence agencies. A country's military (or surveillance system) is estimated to be about 20 years advanced in terms of technology (I read this somewhere) available commercially/ publicly. They have the tools/ technology to bypass security systems known/ available commercially. So while we may think that we have a foolproof security system in place, it could well be just a false sense of comfort. If you are online, you can be tracked, you can be monitored.

Most people in this forum, are NOT anti-Google. Instead, they are anti-Tracking. Google is just one company that tracks you because of it's business model. Going Google-less, may actually mean little, if

your intent is to avoid surveillance. Open-source projects, VPNs, etc may just be adding a layer or two to make it difficult to track you, but then none of it is foolproof.

I strongly think that many of the open-source projects could well be products of intelligence agencies or even corporations like Google itself. It is just that they are marketed in a way to make you believe that you are free from tracking/ Google. The reality could be far from it. Even if the code is available for audit, we have to remember:

1. No one (reputed and reliable) is auditing it CONTINUOUSLY.
2. The tools and technology known/ available commercially are not enough to track codes that are built-in using technology that are way more advanced than what is commercially known/ available.

This might sound like a conspiracy theory, but this could well be true.

Also, many apps are often touted as open-source to mislead users. Apps often have closed-source codes, but may include a few open-source libraries and this aspect is misrepresented to give the impression that the app itself is open-source. So this is another thing one must keep in mind.

What do you think?

3 Likes

TheMystic #2 September 21, 2021, 7:58am

ARE PRIVACY CONCERNS OVERRATED?

The single most important, most debated subject of being online - privacy and security.

While security is undisputed, privacy aspect is.

So what exactly is the concern? As normal people in normal professions (which is easily more than 90% of the population), is there a need for worry?

For a long time since I started using smartphones, I had a natural inclination towards remaining anonymous and private online. I would always use incognito browsing for everything I do online, never create an account with a service as much as possible (e.g. I would watch YouTube videos without signing in), etc.

With time, I began realizing that I am actually missing out on so many interesting things that matter to me, and much of the content that would interest me would be made available to me without much effort using machine learning and artificial intelligence, an area where huge investments are being made.

So slowly I started accessing content and using services with my Google account. Over time, everything from Google feed to YouTube videos were showing me content that I am interested in, and sometimes they were so intelligent that I have been amazed with the whole technology that is at works. Surely, you cannot expect a doctor to give you the right prescription without giving him complete details about your problems. You can't talk privacy there. So **unless the system learns what you like and what you don't, there is no way it will present stuff (including ads) that will be interesting to you.**

With that said, why are are we overemphasizing this aspect of our lives? Is the privacy lobby inflating the privacy problem more than is necessary? Especially since much of what Google learns (according to them) about you is private, and only you can access/ control it, and also because the open-source alternatives are overrated. I say overrated because there are no audit reports (from trustworthy audit entities) available. Their codes may be available for audit, but is there a trustworthy source that is actually auditing them? Are the platforms where they are available being audited? So the issue of privacy and security applies to these platforms too, and more so because they aren't scrutinized as heavily as Google products and services.

As far as more personal info is concerned, like location, age, gender, searches I perform, accounts, mobile number, etc - Google already has all those because I provided them with much of that info when I created my account. Sure, one can always provide fake info for some of them. But if you use 'Find my Device', you are pretty much giving away your location to Google REAL-TIME. While this can potentially be misused, how else is Google supposed to help you if you were to lose your device? Mobile numbers and email addresses are necessarily required to be correct because they are needed when you are locked out of your account. They are the only means to get your account back.

While I am a strong proponent of privacy, I also feel that too much is made out about a lot of stuff that aren't really something to worry about. Those stuff are essential to get the service we expect in return, in other words, putting technology to use.

That said, it is still important not to give anyone a free hand over data, and there has to be several layers of checks and balances, and accountability for safeguarding and using them.

All that said, my current position is this. Make best use of the technology at hand, because if you don't provide the necessary inputs, there cannot be a proper output.

As with some things that we do online which we might want to keep completely private, use a non-google browser (like Firefox Focus or Duck Duck Go) in incognito mode with Duck Duck Go search engine. An even better alternative would be to use a dedicated device with it's own SIM.

1 Like

adrianmalacoda #3 September 21, 2021, 5:59pm

The point of **free software** is "the four freedoms" a.k.a. the freedom to inspect, share, and modify the software running on your hardware. Privacy, security, tracking, ads, etc. are secondary concerns. Anyone who told you free software is "about privacy" is sadly misinformed. The free software movement came about 40 years ago when **a man wanted to fix a printer**.

Personally I am not "anti-Google" in as much as I am anti proprietary software industry (Google, Apple, Microsoft, etc. included). I'm not so much "anti-tracking" (I actually think there is actual or potential FUD about "tracking" in the privacy community (e.g. people don't really distinguish between helpful tools like loggers and crash reporters from adware and analytics libraries)) but privacy and security are more complex than "just use privacy-oriented FOO instead of regular FOO" or "just scan FOO with this magic tracker detector." If an intelligence agency is after you then you need to do far more to protect yourself.

As for your allegations that there may be spyware hidden inside free software, until you name names that is nothing more than FUD. If you have actionable proof of such please show the evidence. As far as I am aware, every time a major free software project has been shown to have spyware (e.g. Audacity) the community has reacted appropriately.

There *have* been intelligence operations against “privacy conscious” individuals, such as **the ANOM operation**, but I don’t know if these involved free software. The ANOM device was a locked down Android device with a backdoor that, importantly, none of its users/targets could inspect or modify. I’m also reminded of **this analysis of how the FBI infiltrated the plot to kidnap the Michigan Governor in 2020** - they were all using encrypted messengers, right? But they had an FBI mole in their midst the entire time, so no privacy-oriented knick-knacks could save them.

2 Likes

adrianmalacoda #4 September 21, 2021, 5:58pm

Re. your second post, I think this assumes that such “services” are desirable or necessary for the user or for humanity. You mention the Google/YouTube algorithms for example, and I disagree with that assumption. I don’t trust mysterious algorithms to always provide the best results or to have a positive effect on the community; I am often disturbed when fellow users are advised to “just use Google” to find an answer instead of answering it or even pointing towards an FAQ. You don’t know what the algorithm will give you or the person you are suggesting that to, you are just blindly trusting it.

The YouTube algorithm in particular has been known to be problematic **and still is in 2021**.

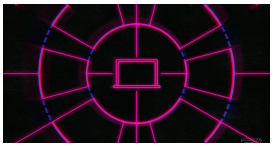
1 Like

Tryder #5 September 21, 2021, 7:33pm

I don’t think one could say the entire open source community is a conspiracy, but I believe it remains true that many of the people governments around the world find, shall we say, troublesome are members of the open source community or otherwise users of open source software. It is therefore obvious that open source software is a target of nation state backed sabateurs working to undermine security in open source projects.

We’re talking about government agencies with near limitless resources at their disposal who have trained agents capable of fooling the most sophisticated counter-intelligence methods in the world. If a Russian agent can infiltrate the CIA or an American agent can infiltrate the BND what chance does a ragtag band of like minded open source volunteers have in identifying an intelligence agent in their midsts?

As demonstrated by researchers at the University Minnesota, it is possible to introduce known security vulnerabilities to the Linux Kernel by concealing them over a series of submissions and spreading them out over multiple areas of the kernel. Individually the submissions pose no threat, but when combined they produce vulnerabilities.



University of Minnesota banned from contributing to Linux kernel

The ban results from research a team was doing.

UMN was banned from contributing to the Linux Kernel over this, but the truth is there's nothing the Linux or open source community can do to combat this type of attack. The resources required to successfully defend yourself from nation state backed sabateurs is astronomical. The wealthiest, most advanced and capable organizations in the world cannot successfully prevent infiltration.

This is hardly limited to the open source community. If they can infiltrate the GRU what makes you think they can't infiltrate Microsoft or Google?

In conclusion, I do not believe Linux, Windows, Android or iOS are government sponsored trojan horses, but I'd be fooling myself if I thought nation state backed organizations around the world haven't been meddling with them.

P.S. If I were a betting man I'd guess Google, Apple and Microsoft are positively teeming with nefarious actors. Not all of them playing on the same team either.

That doesn't mean I think you should throw in the towel. If they're trying to hang you make them work for it.

TheMystic #6 September 21, 2021, 7:51pm

The point of free software, as per your link, is a very noble idea. But without a revenue cum profit stream, I don't see why someone would invest (both time and money) in such solutions.

Personally, I'm neither against paid solutions, nor am I against proprietary solutions. Every maker has the right and freedom to determine the price of his creation. However, I am completely against locking down products after the sale! In other words, I am strongly in support of the Right to Repair movement, which is trying to stop large corporations from owning the products they have already sold. The large corporations should know that they have 'sold' the products, and not leased them for a perpetual revenue stream.

I'm not alleging that spyware is hidden inside all free software. I'm saying that such a potential exists and can be easily exploited. Intelligence agencies and large corporations may easily infiltrate FOSS projects and platforms like F-Droid with their own apps disguised as open source, that cannot be audited properly with the 'dated' tools and technology that these platforms have.

I'm aware that intelligence agencies may plant their own men among criminals to keep track of what they are planning to do. But that is just one way to do it.

But as I described in the OP, the technology and tools available with intelligence agencies are way superior to what is publicly available, and more importantly much of it is unknown too. So while we may

think that the current encryption technologies are fail-safe, they may actually not be so for the intelligence agencies. They may be able to break into the encryption much faster and easier than we think they can.

As with the 2nd post (or 1st comment), it is true that the services are ‘desirable’, though not necessary. Algorithms can be manipulated to feed someone with content that ‘they’ want them to know, or be brainwashed into knowing. I acknowledge that after a point, they have the ability to influence the way one thinks and acts. So it is always advisable to use such services in a very limited way.

1 Like

TheMystic #7 September 21, 2021, 8:00pm

I didn’t imply all of open source community. May be I should have worded my post better to remove ambiguity.

The post only refers to the possibility of apps, or even platforms being actually funded or even founded by intelligence agencies or large corporations themselves.

And platforms like these are more of interest to the surveillance systems because those who come here are usually ones who don’t want tracked. While there may be completely genuine (or nothing illegal) reasons for doing so, such platforms are often also used by members who are often ‘persons of interest’ for governments/ intelligence agencies.

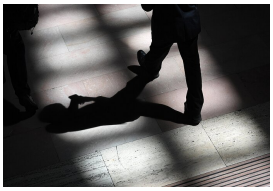
The open source community isn’t as funded as large corporations. So they are easy to break into.

Tryder #8 September 21, 2021, 8:37pm

Any app, corporation, person or organization bears with it the possibility of being more than meets the eye. There are no safe spaces or obvious indicators, you just have to roll the dice and hope for the best.

It’s dangerous out there. Just getting out of bed in the morning you put yourself at risk of tripping over the shoe you left in front of the staircase in your drunken stupor the night before, taking a nasty spill down the stairs and breaking your neck, but you can’t live in fear.

No matter what happens, you’re going to die sooner or later, might as well make the best of the time you have.



Exclusive: Inside the military's secret army, the largest undercover force ever

Thousands of soldiers, civilians and contractors operate under false names, on the ground and in cyberspace. A Newsweek investigation of the ever-growing and unregulated world of "signature reduction."

> “The force, more than ten times the size of the clandestine elements of the CIA, carries out domestic and foreign assignments, both in military uniforms and under civilian cover, in real life and online, sometimes hiding in private businesses and consultancies, some of them household name companies…”
>
> “The newest and fastest growing group is the clandestine army that never leaves their keyboards. These are the cutting-edge cyber fighters and intelligence collectors who assume false personas online, employing “nonattribution” and “misattribution” techniques to hide the who and the where of their online presence while they search for high-value targets and collect what is called “publicly accessible information”—or even engage in campaigns to influence and manipulate social media. Hundreds work in and for the NSA, but over the past five years, every military intelligence and special operations unit has developed some kind of “web” operations cell that both collects intelligence and tends to the operational security of its very activities.”

TheMystic #9 September 21, 2021, 9:21pm

> Tryder:
>
> Any app, corporation, person or organization bears with it the possibility of being more than meets the eye.

Absolutely. And that is the point of the OP.

Most users seem to think FOSS is the solution. But it could well be the unknown angel that is worse than the known devils.

Tryder #10 September 21, 2021, 9:52pm

I agree, many people think that FOSS is the solution, but it’s not really any less likely to be compromised. Although I wouldn’t say that commercial is better or worse. My guess is, and this is just a guess, that one may be better in 2021 while the other is better in 2023 only for the whole thing to flip again in 2024.

So, in that respect, you’re probably best using a mixture of FOSS and commercial and, if you don’t mind the hassle, changing it up periodically. Maybe using Windows in December and Debian the following March then Fedora combined with the Brave browser then Firefox followed by Vivaldi.

I guess if you’re being targeted specifically the idea might be that it takes time to find, craft and exploit vulnerabilities. By the time they’re ready to attack your Windows system you’ve moved on to Debian. Of

course that's a pretty big pain in the buns so, you know, how much are you willing to effect your quality of life I suppose.

At any rate, no level of code transparency, secrecy, oversight or security measures will ever keep you safe from prying eyes or nefarious actors. What you want is a world where you don't need address space layout randomization, 2048-bit encryption or trusted platform modules because no one is trying to steal your information or silence your dissent.

We're not really allowed to talk about that though.

1 Like

tomek87 #11 September 22, 2021, 2:05am

In my opinion, you are talking about something that you don't even understand yet, because this point is currently running in the background. You are talking about the benefits being higher than the costs. Yes they are, but only because you do not bear the costs. That will be subsequent generations, which will have to live extremely limited due to your views. You completely disregard the consequences that this data collection will bring. You can already see what the future will look like in China, where whole ethnic groups are ethnically excluded by algorithms, just like individuals. And the fact that they want to go in the same direction here shows how envious the West is of China's digital possibilities. Or also how Western IT companies repeatedly try to act against their users. Taking two steps forward and then one step back. Open source is not perfect but the best way to show alternatives…

Translated by deepL

TheMystic #12 September 22, 2021, 5:45am

When I surf through online forums, I find that people consider FOSS as synonymous to anti-tracking, anti-analytics, anti-surveillance. This is an incorrect and highly misinformed view…

The point of the OP is just this: FOSS is just as risky, probably even more, than traditional solutions from large corporations like Google. Unless you personally know the developer, the app you have installed is very much capable of doing the very same things that you wanted to avoid by coming to such platforms.

Continuously switching platforms is an impractical suggestion.

If the nature of your work is such that you have to stay away from surveillance, there is only one solution: Don't use any gadgets or technology. Relying on encryption, TOR, VPNs, etc. won't save you.

TheMystic #13 September 22, 2021, 5:52am

> TheMystic:
>
> in the absence of convincing explanations

You have just done that: a vague comment with no specific, supporting, convincing arguments.

> TheMystic:
>
> As with the 2nd post (or 1st comment), it is true that the services are ‘desirable’, though not necessary. Algorithms can be manipulated to feed someone with content that ‘they’ want them to know, or be brainwashed into knowing. I acknowledge that after a point, they have the ability to influence the way one thinks and acts. So it is always advisable to use such services in a very limited way.

If you had read through the comments, I had said this. Algorithms can be manipulated to influence the way people think and act. So they carry the potential to make one dumb and misinformed. Technology can be used to propagate a false narrative of vested interests.

So people must use them in limited ways and not rely on them completely. Staying away from them isn’t ideal either if you want to be competitive and informed. People must have a clear understanding of risks and must not assume something is safe just because it claims to be ‘free and open source’.

tomek87 #14 September 22, 2021, 11:11pm

I agree with you there, of course. Blind trust is never good. However, it must be emphasized that open source stands for principles that are generally accepted as good. Certainly, the partial lack of support or manpower carries risks. However, nowadays, as much as I don’t like to say it, we have to weigh which risks have the greater consequences for us. And in this weighing, open source software generally performs better. Because sooner or often later, it comes out that code was compromised. With open source code, you at least have the possibility of control, even if very few are able to do so. With your argumentation, you give up this crucial advantage. If you want the appearance of security, you should generally stick to projects that have a broad community.
Open source software is not used for nothing in almost every aspect that surrounds us. Closed systems have no future. As they are an island built on dependency and pseudo-security in an open sea that will be flooded. This is illustrated by the theory of the metaverse 🤣🤣🤣😎

Translated by deepL

raven9 #15 September 24, 2021, 12:56am

A lot depends on whether you are likely to be a target or not. Did Seth Rich ever believe his cell phone location was being tracked by a hit team? Did you know you can turn location services off all day long

because all anyone really needs is your phone's EMEI number to track you?
Speak publically about a controversial topic, attend a demonstration, blow the whistle on corruption on Facebook or Twitter and all of a sudden you are a target for surveillance. Does anyone really think that guy in Afghanistan was hit by a drone strike because they thought he had a bomb in his car? Why would anyone fire a hellfire anti-tank missile at a car parked at a house in a residential neighborhood if they thought there was a bomb in it? Only callous psychopaths who have no regard for human life could do that and they are doing that kind of activity routinely in other countries because they are callous psychopaths. We will never know the real reason why that guy was targetted but you can be sure that he was being tracked by his cellphone. No one believes they would ever do that here. Right.

ctnk #16 September 24, 2021, 2:01am

> raven9:
>
> all anyone really needs is your phone's EMEI number to track you?

anyone? That statement reads as hyperbole. How/when is one's EMEI leaked, and to whom?

This crossed my mind when shopping MVNO sites recently. Some of 'em claimed a compatibilty lookup was not possible (or was indeterminate) based on a device model number & demanded "To check, enter your EMEI". Other sites just reported based on model# (after performing a client-side API call to an **ultramobile.com** database) and offered an XX day no hassle refund in case things (comaptibility, local signal strength) don't work out.

Yes, for a given model#, some devices may be carrier-locked. However, even if schmuck doesn't sign up, the MVNO and partners gain a fresh (ostensibly salable) EMEI+IPaddress (+HTTPRequest metadata) fingerprint.

ctnk #17 September 24, 2021, 2:12am

> TheMystic:
>
> So what exactly is the concern?

my belated, considered, response to this nebulous question:

The loss of, or perceived loss of, personal **agency**.

(search engine bubbling… discriminatory pricing, based on profiling [amazon]…)

HunterOpsec10rules #18 September 24, 2021, 6:36am

This post was flagged by the community and is temporarily hidden.

TheMystic #19 September 24, 2021, 3:59am

> raven9:
>
> A lot depends on whether you are likely to be a target or not.

That's true. I made that clear when I said for most people (over 90% of the population).

Didn't find anything called EMEI. So I guess you meant IMEI.

TheMystic #20 September 24, 2021, 4:02am

Unsurprisingly, all tech companies that control the hardware (particularly chips) and software are US companies. They like to collect data on everyone. No wonder China built their great internet wall.

Tryder #21 September 24, 2021, 4:37am

Your service provider can triangulate your position based off of your signal strength. It's not the most accurate method, but it'll get you to within a few miles if not better. Service providers are certainly not immune to government warrants, but many of them are selling this information now so, you know, anyone with your name, number and a few bucks I guess.

My service provider emailed me some months ago to inform me they were going to start selling user data, although they didn't go into detail over exactly what data or how much they were selling it for.

@HunterOpsec10rules People who have a great deal have a great deal to lose and the more they have to lose the more the fear of losing it consumes them. I'd much rather live my life then spend it worrying where the next threat to my empire is going to arise.

That is to say, if there is someone out there spending their time watching everyone; sounds like a miserable existence to me. That's fear, they watch because they are afraid and so it is that fear that has taken control of their lives.

opensourcefan2016 #22 September 25, 2021, 2:14pm

1. On android there are permisions. If you use a foss app, for example a text editor with zero wifi permisions you are pretty safe from tracking on the apps part. Although storing important notes in plain text can lead you to being comprimised. You can use an offline foss text encryption app then in that situation you really are protected from tracking.

2. Hmm maybe that's why Firefox really stopped letting people use addons on android.

3. Apps like vivalda and chromium or edge. But real open source apps like midori, falkon browser, editor text editor or open source.

4. With a good firewall, encryption from the right people, and apps with good permisions it can be posible to use the internet while minimising most tracking done to you.

TheMystic #23 September 25, 2021, 2:52pm

Removing internet permissions can be done to apps from Google Play Store too. That way even those apps can be blocked from tracking. No need for FOSS apps. However, someone said that apps can still make use of Android Webview or other exploits to connect to internet. Not sure how far this is true.

The whole point of this thread is:

foss IS NOT EQUAL TO zero tracking/ analytics/ surveillance.

People think FOSS is synonymous to the above, but it is not. You have to treat apps from outside the Google Play Store with even more caution.

ctnk #24 September 25, 2021, 5:05pm

> TheMystic:
>
> Removing internet permissions can be done to apps from Google Play Store too. That way even those apps can be blocked from tracking. No need for FOSS apps. However, someone said that apps can still make use of Android Webview or other exploits to connect to internet. Not sure how far this is true.

Yes, the concern toward "Webview or other exploits" is valid.

> . **https://madaidans-insecurities.github.io/android.html**
>
> Firewalls, such as AFWall+ or Netguard, are regularly used on Android to attempt to block network access from a specific app, but these do not reliably work — apps can use IPC to bypass the restrictions. If you cut off network access to an app, it will not prevent the app from sending an intent

> to another app (such as the browser) to make it make the same connection. Many apps already do this unintentionally whilst using APIs such as the download manager.
>
> The most effective way to block network access is to revoke the INTERNET permission from the app like GrapheneOS allows you to do. This prevents abusing OS APIs to initiate network connections as they contain checks for that permission, one example of which is the aforementioned download manager. You should also run the app in its own user or work profile to ensure that it cannot abuse third party apps either.

related discussion here: **https://github.com/GrapheneOS/os-issue-tracker/issues/389**

1 Like

TheMystic #25 September 25, 2021, 6:37pm

> ctnk:
>
> Yes, the concern toward “Webview or other exploits” is valid.

That’s very scary.

> ctnk:
>
> **https://madaidans-insecurities.github.io/android.html**

Very interesting.

One of the biggest reason I use a OnePlus device is because of the built-in firewall in Oxygen OS. Color OS (Oppo) too has the same feature. Hope they don’t remove this feature in their integrated new OS.

Xiaomi devices too have it, but they have deeply integrated it with their Security app, which does a lot of other stuff which are quite unnecessary. Samsung, Vivo and Pixel (and probably Motorola and Nokia too) don’t have that feature.

While the article warns against unlocking the bootloader, it still recommends GrapheneOS. That’s contradictory. I’m anyway against custom ROMs because there is a lot of risk in using them. No one knows the developers and what they have baked into the codes. People are only interested in features, which is very simplistic.

For my use, I am fine without unlocking bootloader and rooting. Stock ROMs are less risky than custom ROMs.

justsomeguy #26 September 25, 2021, 7:05pm

> TheMystic:
>
> While the article warns against unlocking the bootloader, it still recommends GrapheneOS. That's contradictory.

It's probably understood but not explicitly stated that installing GrapheneOS involves re-locking the bootloader and having verified boot…

PS. Some think madaidan is another alias of GrapheneOS' developer but theStinger didn't admit it.

1 Like

SkewedZeppelin #27 September 25, 2021, 7:19pm

> PS. Some think madaidan is another alias of GrapheneOS' developer but theStinger didn't admit it.

They are absolutely not the same person.

1 Like

Tryder #28 September 25, 2021, 9:00pm

> TheMystic:
>
> You have to treat apps from outside the Google Play Store with even more caution.

I disagree here. Just being FOSS doesn't mean an app is absolutely free from malware, but malware is pretty prevalent on Google Play.

ignoramous #29 September 25, 2021, 9:19pm

> apps can use IPC to bypass the restrictions. If you cut off network access to an app, it will not prevent the app from sending an intent to another app (such as the browser) to make it make the same connection. Many apps already do this unintentionally whilst using APIs such as the download manager.

Re: IPC: Apps can only IPC to other apps in a very restricted manner (for example, if other apps have `exported` its components explicitly, or if the other apps are signed with the same keys as the app trying to IPC with it).

Re: Intent to browser: Well, that can be sent even when by any app that does not have `Internet` permission. Unless I am mistaken, removing `Internet` permission of an app (like how GrapheneOS does) does not prevent it from throwing arbitrary `Intents` at apps that do have `Internet` permission (like browsers).

Re: Download Manager: Apps can *abuse* `DownloadManager`, though `DownloadManager` itself can be blocked by the firewall. But yes, removing `Internet` permission of an app does disable it from using `DownloadManager`, whereas a firewall like NetGuard / AfWall+ will not do so since they merely track and block connections *owned* by the blocked-apps (`DownloadManager` is the *owner* of downloads it initiates for other apps too, and hence userspace firewalls may not block even if the download was triggered by a `blocked` app).

> The most effective way to block network access is to revoke the INTERNET permission from the app like GrapheneOS allows you to do. This prevents abusing OS APIs to initiate network connections as they contain checks for that permission, one example of which is the aforementioned download manager. You should also run the app in its own user or work profile to ensure that it cannot abuse third party apps either.

Right: This is one valid approach, but a very limiting one. For example, well implemented firewalls can also let you disable access to an entire range of IP addresses, which a GrapheneOS-like firewall can't.

I guess, at the end of the day, it comes down to, what is it that you want to block. To me, the answer is always "block all outgoing TCP/UDP to IPs except the ones I trust". It is not per-app, since that's too coarse, but I can see why that works for some people. It doesn't work for me.

(*disclaimer: I co-develop a user-space firewall+dns client for Android*)

1 Like

SkewedZeppelin #30 September 25, 2021, 9:45pm

@ignoramous

> I co-develop a user-space firewall+dns client for Android

Why dance around it? RethinkDNS, correct?

Edit: you did this weird dance back here too
https://gitlab.com/fdroid/fdroiddata/-/merge_requests/8536

Edit: I don't mean this in a rude way or anything, I'd rather you just say it out that you are one of the devs.

1 Like

ignoramous #31 September 25, 2021, 11:27pm

You say *dance* and then quickly turn around and point out that you don't mean to be *rude*? May be try using more neutral words to reflect your intentions better.

There's no dance here: I did not mention RethinkDNS because I am not here to promote it by forcing it into a discussion where it isn't mentioned at all.

> Edit: you did this weird dance back here too
> **https://gitlab.com/fdroid/fdroiddata/-/merge_requests/8536**

Okay, I'll bite. What problems do you have with that merge-request? Which dance moves did you not like? Genuinely asking because that merge-request is me trying earnestly to do right by the F-Droid community, and informing them what I knew for 5 months but saw little to no response from Blokada AB employees. All I get in response these days to that merge-request is non-stop abuse.

1 Like

SkewedZeppelin #32 September 25, 2021, 11:47pm

@ignoramous
Whoa there.

I was in favor of that merge myself.
I explicitly myself haven't recommended Blokada and even removed it from my recommendations long ago for other reasons.

RethinkDNS is a neat app and is available on F-Droid, I don't see anything wrong with you giving it a mention.

2 Likes

ctnk #33 September 26, 2021, 1:59am

> TheMystic:
>
> I'm anyway against custom ROMs because there is a lot of risk in using them. No one knows the developers and what they have baked into the codes.

This, as a blanket statement, does not stand.

Right in this topic, SkewedZeppelin (DivestOS developer) is participating among us. LineageOS and DivestOS and CRDroid and several other projects maintain publicly available source code repositories

and they even provide DIY build instructions. I do not want / need / care to “know” the LineageOS team, except perhaps the person who is maintaining the build for the specific device(s) that I am using. Know, as in, know how to contact, and gauge (in advance) how receptive they are toward merge requests.

TheMystic #34 September 26, 2021, 2:41am

While Google Play Store may not be completely free of malware, there is still plenty of safeguards in place, which I believe is much superior to unofficial platforms. It is in that context that I used the term ‘even’ more caution.

TheMystic #35 September 26, 2021, 3:06am

> ignoramous:
>
> Re: IPC: Apps can only IPC to other apps in a very restricted manner (for example, if other apps have `exported` its components explicitly, or if the other apps are signed with the same keys as the app trying to IPC with it).

That’s a little reassuring. Google would have thought about it when designing the OS.

More than downloading, the bigger concern is if local files can be uploaded. That’s because even if an app downloads something, user has a good amount of control on what’s next. Android allows plenty of control via app permissions. Is it the download manager that manages uploads too?

I always block internet access (using OS built-in feature, where available) to apps that shouldn’t need it for core functionality. If the built-in feature is not available, I have to rely on 3rd party firewall like Netguard or Karma Firewall. I have always done this thinking this would prevent the app from connecting to the internet completely. This wasn’t necessarily for blocking ads, but just that apps that require local permissions like storage, contacts, camera, microphone, etc. shouldn’t be misusing them.

Now I see that there are still ways for apps to communicate with their servers despite the methods above. But I hope there are sufficient safeguards in place within every OS to prevent such abuse.

Is there a way to block apps from sending out intents too? Atleast block them from sending intents to the downloads manager, browser, Webview, Google Play Services, etc.?

TheMystic #36 September 26, 2021, 3:12am

Is there anyone auditing those publicly available codes or repositories? And doing it on a continuous basis?

And how secure is the platform where these are hosted?

The concern posted in this topic is how platforms can be exploited by someone who has a malafide intent. Obviously, it doesn't apply to all developers.

ctnk #37 September 26, 2021, 4:07am

> TheMystic:
>
> Is there anyone auditing those publicly available codes or repositories? And doing it on a continuous basis?

If I answer "yes" and "yes" to the above, would you believe me?

Consider: the LineageOS "android_frameworks_base" repository
. **https://github.com/LineageOS/android_frameworks_base**
has 800 child forks. The majority of the forked projects represent folks who are DIY builders (no intent to distribute a further customized ROM). They each have a vested interest in keeping abreast of changes//progress in the parent project, and will regularly browse and read the commitlogs describing each change… and (at the moment, 30 merge requests are open) may be motivated to suggest further changes (or reversions) to the parent project.

> And how secure is the platform where these are hosted?

This is a good (important) question. What do you believe is lacking, security-wise? What additional measures are you inferring might (should) be taken? Are you, as a critic, even aware of what measures are, in fact, already in place for a given project?

> NOT anti-Google. Instead, they are anti-Tracking. Google is just one

this, from the OP, does accurately reflect my sentiment FWIW.

SkewedZeppelin #38 September 26, 2021, 4:34am

> has 800 child forks

Count of forks is meaningless.

- lots of people fork a repo to simply have a copy of it.
- GitHub advertising is/was "fork me" for a while

- some people use forks to make their GitHub more appealing on a resume

> 30 merge requests are open

This is even more meaningless, as LineageOS doesn't accept merge requests via GitHub. GitHub prevents disabling of this option.

Development of LineageOS is done on their Gerrit instance: **https://review.lineageos.org/**
And here is CalyxOS: **https://review.calyxos.org/**
And the upstream official AOSP one: **https://android-review.googlesource.com/**

Overall the general sentiment of many eyes being on the code is impossible to measure.
However we (those of us downstream AOSP) still find things.
ie.

- Sometimes we'll tell each other
- sometimes we'll think its obvious enough that others already saw
- sometimes we'll come across what the other has found
- and sometimes it just sits there unfound.

I had typed some examples, but I don't feel like writing a whitepaper's worth of paragraphs on them.

1 Like

SkewedZeppelin #39 September 26, 2021, 4:38am

> TheMystic:
>
> And how secure is the platform where these are hosted?

This is "the next big issue".
It has become reasonably possible to craft decently secure systems.
However supply chain attacks don't care how many walls you have.

Reproducible builds are one way to improve this, but I've seen some experts say that they are instead a waste of time.

You'll always at one point have to trust to an extent someone or something, because none of us have infinite resources (time or money) to control our entire stack.

1 Like

TheMystic #40 September 26, 2021, 4:40am

> ctnk:
>
> If I answer “yes” and “yes” to the above, would you believe me?

I would be surprised. Can you reveal who is auditing them on a continuous basis? As far as I know, people are simply taking the codes and then modifying it a little to present their own versions. And I also don’t see the motivation behind spending resources in the audit. The custom ROM community of users is a very tiny minority, and as a free product, there is even little motivation.

In the madidan link, it was interesting to read that Lineage (the only custom ROM that I was earlier trusting as safe and reliable) isn’t safe either.

> ctnk:
>
> Are you, as a critic, even aware of what measures are, in fact, already in place for a given project?

No, I’m not.

> ctnk:
>
> This is a good (important) question. What do you believe is lacking, security-wise? What additional measures are you inferring might (should) be taken?

I don’t have a technical background, so I can’t comment. But I’m skeptical because of the enormous potential to exploit free platforms. As they don’t have the funding or resources like large corporations to develop and maintain a secure platform.

SkewedZeppelin #41 September 26, 2021, 4:44am

> TheMystic:
>
> In the madidan link

I’ll quote myself from another platform:

> I strongly disagree with many of their points and can’t stand how many people constantly point to them and parrot them.
>
> That isn’t to say a lot of what they say isn’t correct.
>
> People just putting a square box in a round hole even if what they need is a triangle.

It is the most apt way to sum up their site, without divulging into other unncessaries.

2 Likes

TheMystic #42 September 27, 2021, 4:07am

As a custom ROM developer, what is your motivation behind developing AND maintaining a free software? This is not a question specifically to you, but one directed at developers in general.

Also, it is one thing to note/ discover something by chance, and completely another to do a thorough audit, more importantly a continuous one since we have many instances in the past on how either developers had gone rogue, or they sold their product to a rogue, or their platforms were compromised, etc.

Licaon_Kter #43 September 27, 2021, 6:38am

> ctnk:
>
> **https://madaidans-insecurities.github.io/android.html**

“to break away from Google tracking just buy google hardware, signaling Google that tracking is fine and users want more tracking”
“sandbox, security, etc etc etc, they are great…no, you can’t use them since you can’t control the software”
“netguard, afwall - don’t work, don’t try”

Great article, useless article.

TheMystic #44 September 27, 2021, 10:08am

What is your suggestion then?

justsomeguy #45 September 27, 2021, 11:22am

> A conspiracy?

Words and communication become worthless if we use words carelessly. “Conspiracy” should be changed to something else in your OP.

> “Conspiracy: An agreement between two or more persons to engage jointly in an unlawful or criminal act, or an act that is innocent in itself but becomes unlawful when done by the combination of actors.”

(**https://legal-dictionary.thefreedictionary.com/conspiracy**)

None of your “Key Points” alleges any sort of illegality AFAIK. Therefore, you should change the title of your OP.

The real privacy conspiracy: I wanted to link you to an interview of Nicholas Merrill where he explains how the US government’s Patriot Act was unconstitutional, and would be found to be so by US’ courts, if not for legal maneuvering to keep any cases from getting to the Supreme Court (and because few people are willing to stand up for their constitutional “rights”).

However, Youtube/Google again would not grant me access, without surrendering my anonymity (Tor Browser).

> Our systems have detected unusual traffic from your computer network. Please try your request again later. Why did this happen?
>
> IP address: xxx
> Time: 2021-yyy
> URL: **https://www** dot youtube dot com/

So it’s up to you to get G’s help finding it if you wish.

> As with some things that we do online which we might want to keep completely private, use a non-google browser (like Firefox Focus or Duck Duck Go) in incognito mode with Duck Duck Go search engine. An even better alternative would be to use a dedicated device with it’s own SIM.

You are mistaken if you think “incognito mode” is all it takes to be private. It’s obvious you have not even read (or understood) what mozilla says about what incognito mode does and does not do. From everything else (TL;DR), it’s surprising you don’t think DDG is a fake front for Google. It could be… As for another device with another SIM, are you actually trying to give bad advice here?

Licaon_Kter #46 September 27, 2021, 12:52pm

Dunno, better advice in line with reality (or Pixel availability, or price)?

Solutions for users that can’t unlock?

Solutions for users that don’t have one of the supported 6 (six!) devices, but can unlock?

You already know what I mean…

TheMystic #47 September 27, 2021, 1:39pm

> justsomeguy:
>
> None of your “Key Points” alleges any sort of illegality AFAIK. Therefore, you should change the title of your OP.

Key points that were summarised are about the post itself, which was subsequently elaborated and discussed. Therefore, there is no need to change the title.

> justsomeguy:
>
> Words and communication become worthless if we use words carelessly. “Conspiracy” should be changed to something else in your OP.

That’s true, but incomplete. Words and communication can appear worthless when the reader isn’t understanding them too.

In your own words:

> justsomeguy:
>
> it’s surprising you don’t think DDG is a fake front for Google. It could be…

It could be. Just as F-Droid could also be one such front…In which case, this is indeed a ‘conspiracy’. So by definition (including the link you quoted), the term has indeed been used correctly.

> justsomeguy:
>
> You are mistaken if you think “incognito mode” is all it takes to be private. It’s obvious you have not even read (or understood) what mozilla says about what incognito mode does and does not do.

I’m not. I’m fully aware of the limitations of incognito browsing. The reason I mentioned it is to keep that particular activity separate from the normal stuff, to minimize tracking. Also, all that is for people who have hardly anything to lose if those activities were to be actually discovered by someone else, which in other words mean that there is nothing ‘illegal’ about it.

> justsomeguy:
>
> As for another device with another SIM, are you actually trying to give bad advice here?

No. Why is that bad advice? That suggestion is indeed a way to beat device fingerprinting.

ignoramous #48 September 27, 2021, 5:09pm

> SkewedZeppelin:
>
> RethinkDNS is a neat app and is available on F-Droid, I don't see anything wrong with you giving it a mention.

Thanks. Sorry for being abrasive. My interactions ever since that merge-request with the community has been bitter-sweet. For ex: **https://archive.is/H7BPd** (on reddit, albeit)

> SkewedZeppelin:
>
> even removed [Blokada] from my recommendations long ago for other reasons.

Interesting. For what reasons, if I may so ask, especially when **PrivacyInternational** and **ExodusPrivacy** continue to endorse it? (:

> TheMystic:
>
> More than downloading, the bigger concern is if local files can be uploaded. That's because even if an app downloads something, user has a good amount of control on what's next. Android allows plenty of control via app permissions. Is it the download manager that manages uploads too?

Apps downloading stuff is as much a threat, since most 0day exploits are "downloaded" onto the device.

Android's sandbox is as good as its permission model (TOFU aka trust on first use), which has been repeatedly exposed and abused. At least it isn't the nightmare that Windows once was, especially given Android is installed on 3B+ devices world-wide, a scale Windows never reached.

Exfiltration of data (aka uploading without consent) is a concern, but you'd need a good firewall in place and continuously monitor traffic. For me, app-level monitoring doesn't work. What works is blocking all TCP/UDP outgoing connections by default except the ones I allow (note: Exfiltration could also happen over IPSec/ESP, ICMP, and DNS; so the attack surface is really beyond the scope of most firewall implemenations).

> TheMystic:
>
> Is there a way to block apps from sending out intents too? Atleast block them from sending intents to the downloads manager, browser, Webview, Google Play Services, etc.?

Yes, and you do not even need `root`, I believe. **AppManager on F-Droid** can help "firewall" intents and `exported` components in various apps (like `activitys`, `recievers`, `services`, and `content resolvers`).

> TheMystic:
>
> Now I see that there are still ways for apps to communicate with their servers despite the methods above.

Depends on your threat model, really. Just because apps can bypass a firewall doesn't mean they do. It is lot of work and the app would need to be built like a literal `malware`. Of course, user-space firewalls cannot defend against a determined attacker who's willing to put in the time and resources to compromise various defenses (think: NSO's Pegasus) but that does not mean you do not use one. Discarding credible defenses is like reasoning: since my password can be stolen if my browser is compromised, I'd rather not keep a password at all. What's needed is *both* a password and a secure browser.

Licaon_Kter #49 September 27, 2021, 5:29pm

Not sure why one NEEDS to NOT block Download manager. I actually find that it's rarer for apps to use it as opposed to straight connecting.

Too bad there's no "INTERNET permission revoke" without a full system recompile, eg. Use custom ROM

Tryder #50 September 27, 2021, 5:52pm

This is a breakdown of the hidden post made by hunterOpsec10rules. The post makes references to people in the Newsweek article about an undercover army employed by the pentagon I linked to earlier; namely humint, short for human intelligence; and opsec, short for operation security.

The post is written in a strange manner for several reasons. To people other than the target, they're not sure what to make of it and just ignore the post entirely. The target has already been conditioned to believe he's been contacted by a higher intelligence, in this case probably aliens. The odd language used serves to reinforce the target's belief that this message is otherworldly.

> HunterOpsec10rules:
>
> I think I'm in mode be paranoid for [Zero day]

[Zero day] is the day the target believes he is supposed to make his big move. It is not likely that the target has ever been given a date, instead vague references, such as zero day, are made to give the target a sense that there is a day in which he is supposed to make his big move, however, unbeknownst to the target, it is up to him to come up with this date on his own.

The target likely believes he's been able to piece together bits of information left for him here and there to reveal the date, but actually he just came up with it himself. A date was not supplied because it doesn't matter when the target makes his big move, he hasn't actually been contacted by aliens and zero day is not the day he makes his big move against, probably what he believes to be the Illuminati in this case, but the day he gets shot and killed by the police as an active shooter in what everyone else will see as just another lunatic mass shooting.

Additionally, not supplying a date serves to sever any evidence trail. Supplying the date would link the post to the crime. As it is, to everyone else, it just looks like some weirdo posted some weirdo shit.

> HunterOpsec10rules:
>
> command kill Humint, Osint , smartphoting

The target is being instructed to kill humint, human intelligence agents. I'm not sure about the Osint, possibly operation security agents, or smartphoting, but it probably makes sense to the target and his handlers.

> HunterOpsec10rules:
>
> True Argument spy everywhere

Where can the target find human intelligence agents? Everywhere. The target believes spies are virtually everwhere. He's being instructed to go on a shooting spree killing random people, although he believes these people are spies employed by:

> HunterOpsec10rules:
>
> the Illuminati watching everyone

Even the username is part of the trigger "hunterOpsec10rules." Operation Security hunter. I don't know what the 10 rules is in reference to, but I'm sure it makes sense to the target.

This post is a trigger meant to instruct someone to initiate a mass shooting event, although the target believes he will be killing Illuminati spies at the behest of a higher intelligence. The target probably believes this higher intelligence will protect him during his mission, but will, in fact, just be shot dead or otherwise jailed as a madman.

I couldn't say why this person has been targeted for elimination, I don't know who the target is, but I hope he's reading this.

Morgoth #51 September 27, 2021, 7:58pm

What the fuck dude. I really didn't understand it all. Please I need more elaboration or context.

> **Urban Dictionary: fnord**
>
> A fnord is a propaganda word conditioned in the masses from a very young age to respond to, usually with fear, anxiety, or uneasiness, but unable to be seen by the general populace. (This definition originates in the Illuminatus trilogy of books by...

It seems trolling to me, idk

ignoramous #52 September 27, 2021, 11:47pm

> Licaon_Kter:
>
> Too bad there's no "INTERNET permission revoke" without a full system recompile, eg. Use custom ROM

Custom ROM doesn't account for the fact that OEM has many firmware bits running with higher privileges outside of Android itself.

I wrote about it on Hacker News here: **https://news.ycombinator.com/item?id=28627672**

Custom ROM cannot offer privacy… Far from it. Hopefully, PINE64 and Librem become serious enough alternatives.

1 Like

Morgoth #53 September 28, 2021, 12:05am

> ignoramous:
>
> Custom ROM cannot offer privacy… Far from it. Hopefully, PINE64 and Librem become serious enough alternatives.

I would like to have a PinePhone, I don't care about hardware perfomance in general, but battery life is a no-go for me, sadly.
I hope they eventually add 4000mAh battery with similar price.

1 Like

SkewedZeppelin #54 September 28, 2021, 12:12am

@TheMystic

> what is your motivation behind developing AND maintaining a free software?

Personally:
I do it for myself first because nothing provides what I want the way I want it.
Further I already benefit on the mountains of FOSS, why not make it available the same? Why should it sit on my hard drive only to be used by myself?
Lastly, I myself always try to use FOSS whenever/wherever possible, why would I make something proprietary?

@ignoramous

> Custom ROM doesn't account for the fact that OEM has many firmware bits running with higher privileges outside of Android itself.

It is an issue, but can be managed given reasonable expectations.
I'd far rather see PinePhone and Librem support AOSP first.
Linux on mobile is too far away to be usable and F-Droid already has over 3,000 FOSS designed-for-mobile apps.
And Linux desktop security is currently far behind what AOSP provides, such as extensive compile time hardening and aggressive isolation of all services and apps.

> Custom ROM cannot offer privacy… Far from it.

Strong disagree. That is too defeatist.

I say this as someone who both maintains a "deblobbed" ROM and helps support the leading Linux desktop sandbox utility.

1 Like

Licaon_Kter #55 September 28, 2021, 6:47am

Integrated firewall to revoke INTERNET is a step forward, why keep on moving the goalposts for every answer? Yes, you are right…but…

TheMystic #56 September 28, 2021, 6:54am

> ignoramous:
>
> Apps downloading stuff is as much a threat, since most 0day exploits are "downloaded" onto the device.

Can mere downloading of something be a threat? I thought, on Android, as long as ‘unknown sources’ are disabled, there is very little a downloaded file can do.

> ignoramous:
>
> What works is blocking all TCP/UDP outgoing connections by default except the ones I allow

How does the average user configure this?

> ignoramous:
>
> Yes, and you do not even need `root`, I believe. **AppManager on F-Droid** can help “firewall” intents and `exported` components in various apps (like `activitys`, `recievers`, `services`, and `content resolvers`).

I tried this app. For most apps (actually almost all of them) that I tried to block trackers, it gave me the error ‘Could not disable trackers’. I am using OnePlus device with OOS 11.0.9.9, not rooted.

I also checked ReThink DNS. It is a little complicated and time consuming to setup.

Here is my requirement:

1. Block all sorts of trackers and ads from all apps.
2. Block internet access to apps I choose.
3. Block intents for apps I choose (e.g. a gallery app should just show me the pictures and videos on my device. There is absolutely nothing more it should do or be allowed to do)

Is there really a solution? Preferably a non-root solution.

For the sake of simplicity, we can ignore the possibility of a determined hacker, and therefore a super-hardened security solution is unnecessary in my case (also true for most users too).

TheMystic #57 September 28, 2021, 7:02am

> ignoramous:
>
> Custom ROM doesn’t account for the fact that OEM has many firmware bits running with higher privileges outside of Android itself.
>
> I wrote about it on Hacker News here: **https://news.ycombinator.com/item?id=28627672**
>
> Custom ROM cannot offer privacy… Far from it. Hopefully, PINE64 and Librem become serious enough alternatives.

I guess it is impossible to use technology without being tracked.

"Replacing OEM Android is only one part of the equation. There are many components that run with full privileges (EL2/EL3?) outside of Android and never subject to Android's sandbox. Well, at least until Google can force OEMs to stricter standards with their effort to KVMize those privileged executables [0].

If you do not trust the OEM, replacing its ROM with GrapheneOS / CalyxOS / LineageOS isn't going to help much anyway.

One right answer to this is fully open-source (hardware and software) phones like the PINE64 and Librem, among others."

Even if you take care of the software/ firmware, you still are using the same hardware (e.g. the chips used in the device) that can spy on you. For example, how iPhones can keep track of location even when switched off.

TheMystic #58 September 28, 2021, 7:09am

> SkewedZeppelin:
>
> Personally:
> I do it for myself first because nothing provides what I want the way I want it.
>
> Further I already benefit on the mountains of FOSS, why not make it available the same? Why should it sit on my hard drive only to be used by myself?

Appreciate that. I also read through some of the comments in your OS post where you made it clear that you do not want obligations (which happens when you put a price for your product).

> SkewedZeppelin:
>
> Lastly, I myself always try to use FOSS whenever/wherever possible, why would I make something proprietary?

I don't know why, but i am increasingly suspicious of everything free (since there are no free lunches). I am more inclined to think that going anti-Google is basically handing over your data to another entity, who can do pretty much the exact same things that you wanted to get away from. Besides, it is very much a possibility that the new entity is actually the same old entity in a disguised form.

TheMystic #59 September 28, 2021, 7:11am

> Licaon_Kter:

> Not sure why one NEEDS to NOT block Download manager. I actually find that it's rarer for apps to use it as opposed to straight connecting.

I think most apps rely on the system download manager. So blocking it will prevent the downloads too.

Licaon_Kter #60 September 28, 2021, 7:40am

Depends on *your* apps, yes,

Browser? Email client? Chat app? Osmand? None use it…

Looking at my allowed hosts: organicmaps (not using it), trekarta (for a bug test) and radiocells (if I remember to update it once a year)…nothing else

Tryder #61 September 28, 2021, 9:46am

How might a person come to believe that a higher power is communicating with them? Take the religious type as an example. Religious people tend to think that god might communicate with people through "signs," which is to say events in a persons everyday life.

As an example, let's say someone was thinking about proposing to his girlfriend. As he's thinking about this on his daily commute he passes a bus with an ad for a wedding chappel and thinks to himself that this was a sign from god that he should pop the question.

Now, if you wanted someone to think that you were god all you have to do is communicate with them in this manner. So let's return to our marriage example and say you're a well funded, well connected organization and you wanted the guy from the above example to get married so you bought ad space on a bus you knew he would pass on his way to work.

To really hit the message home you also bought ad space on a park bench near his apartment. On his way home the guy contemplating marriage was also cut-off by a car with the license plate "gotspouse," that might be too many characters for a license plate, and maybe a few other things.

Of course you knew he was thinking about getting married because you had access to his internet search records and browsing history and knew that he had recently searched about marriage failure rates and the cost of engagement rings. You also had access to his location history, call history, contacts, social media presence, etcetera so it's not too hard to develop a picture of the things going through his mind.

Once the subject is under the belief that a higher power is communicating with him he's basically putty in your hands. He'll do anything you say without question. So if you want finer control over his actions you can start communicating with him more directly.

For instance, you might pay an actor or social media influencer to say something on Facebook then share that message to the target's social media feed. To the social media influencer the message looks like a plug for some product, but to the target it's part of a broader campaign to steer his world view.

Maybe the plug says something like "so good even the Illuminati can't resist." The influencer thinks it's just a stupid crack about conspiracy theorists, but the target sees it and thinks "man I'm seeing Illuminati stuff everywhere I go lately."

You write articles and pay to have them published on websites the target is known to frequent. And finally you start indirectly posting cryptic messages to him on forums he's known to frequent.

justsomeguy #62 September 28, 2021, 11:14am

> It could be. Just as F-Droid could also be one such front…In which case, this is indeed a 'conspiracy'. So by definition (including the link you quoted), the term has indeed been used correctly.

AFAIK there is nothing illegal about creating companies but not publicizing the true ownership. That said, the history of F-Droid makes that seem unlikely. It's hard to even argue civil damages or fraud, because you don't give a dime to any of them as a "purchase." If it's not illegal, it's not a "conspiracy." Wrong word.

DuckDuckGo says they use Amazon affiliate links. If you buy something, Amazon knows who you are. Amazon sells or shares or trades your info'. Legal. Tracked…

> No. Why is that bad advice? That suggestion is indeed a way to beat device fingerprinting.

Devices and SIMs are usually connected with individual identities AFAIK. It doesn't matter if you use 2 or 10 different devices, unless you take care to not connect them with your identity, which isn't trivial.

ctnk #63 September 28, 2021, 1:29pm

> justsomeguy:
>
> AFAIK there is nothing illegal about creating companies but not publicizing the true ownership.

Certain countries/juridictions prohibit it, e.g. Germany, right?

TheMystic #64 September 28, 2021, 4:00pm

> justsomeguy:
>
> AFAIK there is nothing illegal about creating companies but not publicizing the true ownership. That said, the history of F-Droid makes that seem unlikely. It's hard to even argue civil damages or fraud, because you don't give a dime to any of them as a "purchase." If it's not illegal, it's not a "conspiracy." Wrong word.

You don't seem to understand the difference between withholding information and misrepresenting information. Withholding information isn't illegal (e.g. SurfShark VPN doesn't disclose to the public/ users who their owners are), but misrepresenting information is illegal. Fronting is misrepresenting information, and is illegal. And fronting is a conspiracy. So RIGHT word.

> justsomeguy:
>
> DuckDuckGo says they use Amazon affiliate links. If you buy something, Amazon knows who you are. Amazon sells or shares or trades your info'. Legal. Tracked…

Amazon selling or sharing info isn't DDG's fault. Amazon only gets the order. DDG doesn't (or shouldn't) tell Amazon what else that user does on DDG. Amazon only knows that the user they are serving placed the order via a DDG affiliate link. This is assuming that DDG doesn't track or share that info.

> justsomeguy:
>
> Devices and SIMs are usually connected with individual identities AFAIK. It doesn't matter if you use 2 or 10 different devices, unless you take care to not connect them with your identity, which isn't trivial.

You connect to internet either via WiFi or Mobile Data. WiFi gives away a lot more information than mobile data. WiFi location is mostly fixed. WiFi also (like SIM) is tied to an identity, either the individual himself or a family member (in most cases). There is much more fingerprinting possible when using WiFi.

So using a dedicated device with its own SIM, and obviously without logging in with a real identity, adds to the security/ privacy, even if it isn't a way to stay away from tracking completely (which is impossible if you use internet).

justsomeguy #65 September 28, 2021, 5:42pm

> misrepresenting information is illegal

If misrepresenting information is illegal, then we shouldn't be using aliases or sockpuppet accounts, or implying FOSS developers are doing anything illegal, based only on hypothetical FUD.

You also shouldn't be telling people to buy a dedicated device with its own SIM to use for "some things that we do online which we might want to keep completely private". That by itself only helps the monitors more easily separate the wheat from the chaff.

1 Like