Avoiding "The Botnet" - impossible?

Introduction

People these days worry more and more often about escaping what I will call "The Botnet" in this article - just a "meme" way of describing mass surveillance. Websites have been created describing spyware and alternatives to it. Replacements for social services, instant messaging, VoIP, etc. already exist. You can use anonymizers like the TOR network or a VPN to hide from your ISP. There are ways to privately share files and host websites as well. But are all those effective - and more importantly - **is this the core of the botnet** - or maybe we're going after this entirely the wrong way?

Existing ways of combatting The Botnet - and why they're ineffective

VPNs

These are proxies that route ALL traffic (not just HTTP) through their servers. There are lots of them claiming to be 'no log', but it is easy to find examples where people got ratted out by these, like https://www.wipeyourdata.com/other-data-erasing/no-logs-earthvpn-user-arrested-after-police-finds-logs/ (archive). Even assuming the 'no log' policy is true, the government could still possibly legally force the provider to track someone (at least in certain countries where that's allowed). If that's not an option, there's always the old raid them and steal the servers (archive) (MozArchive) tactic. Of course, VPN traffic is also easily blocked at the ISP or website level.

VoIP, social, IM, etc.

Simply suffers from **lack of usage** - so if you want to actually reach anyone, it's Facebook, Skype, etc. Much of the commonly recommended "secure and private" IM software has various issues (Signal and Telegram require a phone number; Keybase has had a security audit which found many issues (local); Matrix protocol has just had a security issue found (archive)). TOR-based messengers rely on the security of the TOR network, which is analyzed below. Server-based ones, on the other hand, rely on the security of servers controlled by people you don't know. And as usual, it's all going through the enemy's networks. I don't mean to say that all those alternative ways of communication are useless, but that we can't rely on only one layer of protection - the messaging application level.

UPDATE August 2025: this is going to become very obvious soon with the resurrection of Chat Control (archive) (MozArchive), which I was planning to write about earlier, but then it died (archive) (MozArchive), and I was assuming (or maybe just hoping?) it'd stay dead. Not in this cursed world, apparently; the necromancers just can't stop animating their favorite corpse to haunt us all.

When talking about Chat Control, people almost always focus on the horror of breaking encryption, but if you read the actual law (local), you will realize that the problems with it go much deeper than that. For example, **every hosting or communication provider will have to assess the risk** that his service will contribute to the proliferation of child sexual abuse (and do that every year / 2 / 3 according to the risk level). There is a template for this at the end of the document. After that's done, the communication platform will have to perform *“risk mitigation”* which consists of:

- *adapting, through appropriate technical and operational measures and staffing, the provider’s content moderation or recommender systems, its decision-making*

processes, the operation or functionalities of the service, or the content or enforcement of its terms and conditions;

- *reinforcing the provider's internal processes or the internal supervision of the functioning of the service;*
- *initiating or adjusting cooperation, in accordance with competition law, with other providers of hosting services or providers of interpersonal communications services, public authorities, civil society organisations or, where applicable, entities awarded the status of trusted flaggers in accordance with Article 22 19 of Regulation (EU) 2022/2065 …/… [on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC];*
- *initiating or adjusting functionalities that enable users to notify online child sexual abuse to the provider through tools that are easily accessible and age-appropriate;*
- *initiating or adjusting functionalities that enable users to control what information about them is shared to other users and how other users may contact them, and introducing default suitable privacy settings for users who are children;*
- *initiating or adjusting functionalities that provide information to users about notification mechanisms and direct users to helplines and trusted organisations, where users detect material or conversations indicating potential online child sexual abuse;*
- *initiating or adjusting functionalities that allow the providers to collect statistical data to better assess the risks and the effectiveness of the mitigation prevention measures. This data shall not include any personal data.*

In short, every communication platform (which would include tiny XMPP servers like mine)

would need moderators and a ToS; reporting functionality; ability to change privacy settings **and private defaults for children**; links to *"helplines and trusted organizations"* (wtf?); as well as collecting some kind of statistical data (the end of no-logs services like my MUC).

Do you see now how it's not just about breaking encryption? In fact, that's irrelevant now because **the new version of Chat Control explicitly forbids that**. But anyway, did something in the above paragraph catch your attention? Because, to implement the *"private defaults for children"* part, you'd need to track their ages. And that is exactly what the EU requires:

> *Providers of interpersonal communications services that have identified, pursuant to the risk assessment conducted or updated in accordance with Article 3, a risk of use of their services for the purpose of the solicitation of children, shall take, the necessary age verification and age assessment measures to reliably identify child users on their services, enabling them to take the mitigation measures.*

Anyway, after performing the risk assessment and mitigation you have to send the results of that to some *"coordinating authority"* (these are per country). If they decide there is a high enough risk of child abuse proliferation, they will force you to install *"detection technologies"*:

> *The Coordinating Authority of establishment shall have the power to request the competent judicial authority of the Member State that designated it or another independent administrative authority of that its Member State to issue a detection order requiring a provider of hosting services or a provider of interpersonal communications services that are classified as high risk in accordance with Article 5(2) or parts or components of the services classified as high risk that fall under the jurisdiction of that Member State to take the measures specified in Article 10 for the sole purpose of to*

> ***detecting in visual content or URLs the dissemination of online child sexual abuse material on a specific service or parts or components of the service****, classified as high risk in accordance with Article 5(2), for a limited period as specified in paragraph 9 of this Article.*

A little later the gov-boomers expose their lack of familiarity with the relevant technology:

> *Providers of hosting services and providers of interpersonal communications services that have received a detection order shall execute it by installing and operating technologies approved by the Commission to detect the dissemination of known or new child sexual abuse material or the solicitation of children (the 'technologies'), as applicable, using the corresponding indicators provided by the EU Centre in accordance with Article 46.* ***In interpersonal communications services using end-to-end encryption, those technologies shall detect the dissemination of child sexual abuse material prior to its transmission****.*

Obviously - if you're running something like an XMPP server - the bolded is impossible. Gov boomers are assuming everything is like Discord or Signal, where the client and server are the same thing. So, they figure they don't have to care about compromising encryption because they will just grab the data client-side earlier. But, this approach can't be applied to XMPP as the person that controls the server, doesn't control the client. So even if they judge the server as dangerous, they will only be able to apply the general *"risk mitigation"* requirements. Of course, this is still way too much burden for your average XMPP hoster, and will bury him. But at least XMPP servers are truly immune to having to decrypt their users' communications. Yet, can we be sure the spies won't go after XMPP clients on the software repos? After all, they also have a section called *"Obligations for software application stores"* which says that those need to:

> *take reasonable measures to prevent child users from accessing the software applications in relation to which they have identified a significant risk of use of the service concerned for the purpose of the solicitation of children;*

So yeah, software distributors will also have to verify ages. Either way, prepare to have your images scanned on any communication platform where the server and client are the same. And of course, if the users are not running E2EE, the spies can also enforce scanning server-side.

Is it not obvious by now, that we cannot fight the botnet just by installing "NanonChatAppSupreme"? We are now surrounded not only by the big corporations that want to collect our data for profit and lock us into their ecosystems (they are the only ways of communication most people know), but also by states (or multi-state hydras like the EU) that want to bury all alternative platforms with an avalanche of requirements that they cannot hope to fulfill. So, even if you managed to escape the big corpos and dragged your normie friends to XMPP, Matrix or whatever (and you trust your hosts), the second form of the final boss is waiting to devour you while you're out of items and on low HP. This seems very deliberate.

Oh, and if you think "ah-ha! I use [insert messenger that's independent of servers, or can switch them, etc], EU spies can't touch me, hahaha!" then hold it, because this isn't their only way to slither in. Again, if they get a clue in a few years, they could just force the software repositories to modify the binaries or even sources on github to perform client side scanning. They could install spyware on the target devices like they do with journalists already. And I'm sure I'm missing ways. By the way, the new law is a lot longer, but I don't care to even read all of it, as most of it doesn't seem relevant here. There's stuff about the communication provider having to release transparency reports about the results of child abuse investigations, etc. But that's just adding more requirements to an already buried service so...There's also a bit about how, if the

service is hosted outside the EU and ignores pleas for cooperation, they will just block it. Either way, another proof the botnet is physical.

File sharing, hosting...

All regular hosting / file sharing providers have huge lists of what's allowed and what isn't. Even my current host *“reserves the right to suspend, block or cancel access to any and all Services”*, if they decide something contradicts their list. And of course, copyright holders can claim something is violating theirs, and you get your shit deleted then. Rom sites have been getting taken down recently for example. There are also 'good hosts' like autistici.org, but who's to say the government won't eventually take them down if they host too much stuff they don't like? As long as we're using their networks, nothing is safe. Push comes to shove and they raid the servers. Even Freedom Hosting went down eventually.

Operating systems

Alternatives to Windows are available, but you will come across Microsoft's system sooner or later - whether at a relative's house, school (they have deals with those (archive) (MozArchive)), or somewhere else. Not that Linux is all that great either in the botnet department - big corporations like Mozilla or Red Hat (through systemd), still influence it in negative ways. This will happen in any society in which deals based on profit and / or control are prevalent. Edit: and now the legal system is also getting involved.

The TOR Illusion

The TOR network allegedly allows you to browse the Internet anonymously. It works like 3 proxies connected together except encrypted, so a "proxy" (called the TOR node) cannot see the contents of the previous, only the destination. However, the last node **does see unencrypted traffic** - so we hit a roadblock already before we started. The first node also sees your IP, but not the contents of your request.

What are some other problems with TOR? Well, a lot of websites simply block it, or otherwise try to make its usage inconvenient. Since the **list of exit nodes is public**, any website owner can easily do it. So you might be planning to "anonymize your browsing", but then realize it's simply unsuitable for everyday usage. Even more so if you intend to actually interact with the websites you're visiting - forums, imageboards, markets, file download websites, etc. all famously hate TOR. If push comes to shove, **ISPs could very easily block all TOR traffic as well** - in fact this has already happened in Venezuela for example - https://www.accessnow.org/venezuela-blocks-tor/ (archive) (MozArchive).

What about the so-called hidden services - exclusive to the TOR network? Well, most of them are defunct and it's hard to find one that actually works - and if you do, mostly you just see some scraps. In my country, I was only able to find ONE onion forum that I could actually connect to, and it didn't have very much activity. Their servers are also routinely raided (see Freedom Hosting) and their owners jailed.

There are many ways of identifying TOR users anyway - browser fingerprinting, stylometry, or even people sharing their personal data while on TOR. Operation Onymous (archive) (MozArchive) was very successful (though kind of overstated by the feds - the amount of seized sites were "only" 27 - here is a list). An already famous case of a guy sending a bomb threat using TOR can be read here: https://www.bestvpn.com/privacy-news/harvard-bomb-

threat-student-caught-using-guerrilla-mail-tor/ (archive) (MozArchive). They got him because he was the only person using TOR on that particular network at the time. The FBI has even paid a university to deanonymize TOR users (archive), and that's how Silk Road 2.0's owner could be locked up. This is just what we know about - more attacks are surely in use or preparation.

TOR still relies on its encryption, and if that's ever broken - say goodbye to your anonymity, since all the traffic is stored for possible future decryption. Though the TOR network does use Perfect Forward Secrecy, which should ensure the security of the encryption keys (without a direct attack on your device) - cracking the actual ciphers is still a possibility:

> *However, forward secrecy cannot defend against a successful cryptanalysis of the underlying ciphers being used, since a cryptanalysis consists of finding a way to decrypt an encrypted message without the key, and forward secrecy only protects keys, not the ciphers themselves.*

Quantum computing makes this likely, too. Another thing that's absolutely required for the security of TOR (that somehow no one is speaking about) are the **nine trusted-by-default directory authorities**. If a few of those are ever compromised (maybe that's already the case?) all of TOR's advantages **go out the window**. This issue has been analyzed in depth here.

Even the praised TOR Browser is not perfectly safe - for example, just using different buttons in your window manager can expose a different screen resolution (TBB version 8.5.3, newest as of writing). The first theme is Murrine, second - Default XHDPI, if you want to confirm.

Of course, this alone is probably not enough to deanonymize you - but many more issues surely

exist, waiting to be discovered. Put a few together and you might just find yourself exposed. Conclusion? **TOR is not the panacea**. Does that mean you shouldn't use it? No, of course. Use anything that's available to improve your privacy and anonymity - just realize it's not a magic spell, and **does not strike at the core of the botnet**.

UPDATE November 2024: another attack on TOR has recently dropped (archive) (MozArchive). It's quite creative, and it's summarized adequately in this one quote:

> *Could someone be deliberately trying to induce abuse complaints on Tor network participants to take down parts of the network (or disincetivize running internal nodes, which are key for the network's health)?*

The answer is yes:

> *This spoofing "attack" actually started on other types of nodes before migrating to relays, and those other nodes were hit with a much larger volume of spoofed connections, leading to them actually getting temporarily taken down in some cases!*

Of course, this doesn't deanonymize anyone directly, but if people stop running nodes because of abuse reports (which is what I'd assume happens in a significant number of cases), it would decrease the anonymity for every TOR user.

> *You, too, can probably make your friend's hosting provider (with their consent, of course) shut down their server and cancel their hosting contract by getting them flooded with well-meaning but confused abuse complaints.*

Yes, you could. It always comes down to who owns the infrastructure, and who decides the "rules" according to which it runs. That's why we can't win this "war" by installing some type of software on our computers (alone). We need our own server spaces, our own ISPs, ones that keep no logs and ideally require no "contracts" to sign up for. Alternatively, to bypass the ISPs completely. Anything else is a mirage that's destined to disappear anytime an attack like this happens.

Inventing more darknets doesn't do anything

I don't care whether it's i2p or nym. I don't care how advanced they seem at first - weaknesses will be found eventually, like they were for TOR. They all rely on encryption that will be broken eventually. And they are all going through the enemy's networks. A meshnet has a too high barrier for entry (both skills and cost), and doesn't protect against states who have decided that selling meshnet devices will be banned, or the ones that have access to CCTV AI to detect who's using them, the ones who can compromise hardware at the production level (archive) (MozArchive) - *“Behind the scenes, BAC was secretly producing modified pagers containing the powerful explosive PETN, specifically targeting Hezbollah, reported The New York Times.”*, the ones who can put an Alexa in your apartment by default (archive) (MozArchive) to hear what you're doing at all times, the ones who can delete you from existence by zeroing your bank account or throwing you into prison or doing any of the myriad of things that having access to the physical infrastructure lets them. Do you not see now how it all comes down to the physical infrastructure?

The core of internet surveillance

To derive benefit from the Internet's most popular services (like Facebook, Twitter, IM, website hosting), you have to deal with their terrible terms of service and privacy policies. Not only that, but any packet you send or receive is physically going through networks that **you don't control**. ISPs can watch, modify and block them any way they want - and they are subject to government whims as well. Encryption is at best a temporary non-solution, as explained in the TOR section (they could block all encrypted messages easily for example - by comparing them to known languages. If it's not found in any known language, the packet is trashed. Blocking HTTPs? What was it - port 443? Boom and done). Maybe some smart 'hackers' would learn to bypass these blocks, but in the end, we'd be fighting a battle we're sure to lose. Eventually we're going to have to face the fact that...

The Real Botnet...is PHYSICAL

As said, servers for the services we use are owned mostly by big corporations (or sometimes other strangers, which almost always have to submit to the former either way), while ISPs and governments own the networks, so **the botnet is physical**, not technological - and the solution, by extension, must be as well. This might be hard to see in internet surveillance (which is not even the worst botnet) - but easy in something such as CCTV. They come in, mount the cameras, and boom! You're being watched. You're now **their property** - which they literally admit to. No really - for 30 days (or some other amount), they can do whatever they want with your captured movements. And the duration is just claimed...Regardless, you're at their mercy now. If they see you engaging in some 'forbidden behavior', **they can punish you** and they do have a proof you did it. And they can blame you for sins they arbitrarily chose - they certainly **aren't asking you** if something should be banned or not. Everything in this society is owned by businesses or governments - and so serves **their interests**, not yours. CCTV is just one example.

Drones, killer robots, whatever you can think of - and not necessarily technological. Schools, hospitals, airports (remember the patdowns?) - you have **no control** over any of these. And that is **The Real Botnet**. If we want to destroy internet surveillance, we're going to have to take over not only the most popular services' servers (hey, we can have a Facebook that respects the user - no, really!) but also the ISPs - **PHYSICALLY** - since presumably we won't spy on or censor ourselves...And with that, hopefully we can bury the other botnets as well.

The Fake Botnet Fighter

The guy sitting in his apartment wearing a hoodie, running a fully libre ThinkPad, unbreakable Qubes OS, TOR for all connections, carefully avoiding all stylometry and sharing any personal data at all, encrypting his communication with a one time pad three times, and worrying whether some botnet hasn't slipped in anyway. He has no phone or only uses "burner phones" and pays with bitcoins. And then...he finally has to come out of his house, and has his face recorded by a CCTV camera a hundred times. This guy has to be respected for his dedication, but he is useless for a revolution. **You cannot combat The Botnet using tech only.**

All your tech solutions...will eventually fall!

It is inevitable. And everytime it follows the same script - some country or ISP blocks TOR or VPNs, or torrent sites get taken down, or Facebook / Twitter / YouTube implement yet another way of censorship, or any of the myriad of other issues you can think of. People then freak out and scramble for more technological solutions that are **only band-aids**. Then, if they find one, they continue their comfortable life while the cuffs get tighter. I mean, can you imagine that, in 20 years, you will be able to use the Internet as freely as today? Impossible - they will keep

cracking down on everything until the 'solutions' are too tough or not even viable anymore. If we controlled the infrastructure, we could not only delete all logging ISP-wide, but also fix all the problems with FB / YT / other malicious service providers. Of course, you cannot take over just like that - **the web of slavery is too deep** - if we just barged in, the police, media etc. would get involved, and that would be the end of it. **A full-scale revolution is our only option** - and we should use the time during which we can fairly freely talk on the internet to plan for it. Then we could fix not only "The Botnet", but most of the other problems of society.

Linux is a cuck OS now

So you probably heard already that recently, the USA states California and Colorado had installed an absolutely insane law (archive) (MozArchive) which puts extreme burden on OS maintainers, application developers, and distributors. Let's check out a few quotes to see just how insane it is. First, some definitions:

> *(g) "Operating system provider" means a person or entity that develops, licenses, or controls the operating system software on a computer, mobile device, or any other general purpose computing device.*

The developers of big linux distros are public personalities and easily fit this. Many of them are literal companies so there is no escape, and they will be subject to this law, as well. And the *"Operating system provider"* has to...

> *(1) Provide an accessible interface at account setup that requires an account holder to indicate the birth date, age, or both, of the user of that device for the purpose of providing a signal regarding the user's age bracket to applications available in a covered application*

store.

So, anytime you install a Linux (or any other) OS, it's supposed to store your *“age bracket”* so that it can send it to the programs you download from a *“covered application store”*, which might seem like it fits only a repo, but actually...

> *(e) (1) “Covered application store” means a publicly available internet website, software application, online service, or platform that distributes and facilitates the download of applications from third-party developers to users of a computer, a mobile device, or any other general purpose computing that can access a covered application store or can download an application.*

Anyone who distributes a program publicly is subject to this law. Whether this includes torrenting isn't obvious purely from the definition. But, if you have a website on which you make available a binary or exe, or even a bash or python script, you're now inside the net.

> *(b) (1) A developer shall request a signal with respect to a particular user from an operating system provider or a covered application store when the application is downloaded and launched.*

Every application must contain the functionality of sending the age bracket signals (that they receive from the OS they running on, which has to store them).

> *(2) (A) A developer that receives a signal pursuant to this title shall be deemed to have actual knowledge of the age range of the user to whom that signal pertains across all platforms of the application and points of access of the application even if the developer*

willfully disregards the signal.

And since the developer is supposed to receive the signal, **all programs must be phoning home**. Imagine the burden on all the devs that will now have to add mailing functionality to their software...

> *(B) A developer shall not willfully disregard internal clear and convincing information otherwise available to the developer that indicates that a user's age is different than the age bracket data indicated by a signal provided by an operating system provider or a covered application store.*
>
> *(B) If a developer has internal clear and convincing information that a user's age is different than the age indicated by a signal received pursuant to this title, the developer shall use that information as the primary indicator of the user's age.*

Hahaha. If the developer knows you personally, and you are a minor who lies during OS installation, he is required to report that...

> *1798.502. (a) With respect to a device for which account setup was completed before January 1, 2027, an operating system provider shall, before July 1, 2027, provide an accessible interface that allows an account holder to indicate the birth date, age, or both, of the user of that device for the purpose of providing a signal regarding the user's age bracket to applications available in a covered application store.*

OS providers are now required to have autoupdates that will ship this functionality. Also looking at the last bit, the law makes it clear that **the application stores must comply with this**

law, too; as in, they have to accept only programs that ask for the age bracket data. And remember, that means personal websites and every other way of sharing software! What happens if they don't comply?

> *1798.503. (a) A person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars ($2,500) per affected child for each negligent violation or not more than seven thousand five hundred dollars ($7,500) per affected child for each intentional violation, which shall be assessed and recovered only in a civil action brought in the name of the people of the State of California by the Attorney General.*

Hahaha.

So let's recap. Every OS must ask the user to set his age bracket during installation, and save it. Every application must then be sending this data during launch, to the developer that is required to store it. Every repository or other place that distributes software, can only accept those that have this functionality built-in. If any of those entities ignore the law, they will get fucked by a several thousand dollar fine for every kid that uses their OS or program.

This - if properly enforced - **will kill every FOSS operating system**. No one can afford to modify all the applications to support this (remember this includes ls, cd, ping, ssh, and so on). It's the death of the independent software repository, which is unlikely to bother itself with a database to store all the age bracket data, as well as hunt for independent info about their users, deal with government requests, worry of fines, and so on. Linux devs will also now have to ensure their creations contain this functionality, and also to provide contact info, lest their programs won't be included in official repositories. Of course, this doomerism depends on

whether people actually obey. And yet...

- "XDG Desktop Portal" plans on cucking (archive) (MozArchive).
- Kicksecure very proudly cucks (archive) (MozArchive).
- Super secure Qubes will likely cuck, too (archive) (MozArchive).
- Someone who seems to be a NixOS dev said (archive) (MozArchive) - *"In this case I'd let Red Hat and similar ones to take point. And then if those do something which would be meaningful in NixOS, let's consider it. Similarly, if they do not feel like anything is needed, I very much doubt that it makes sense for NixOS to try doing something"*. Therefore, prepared to cuck.
- Elementary OS cucks. (archive) (MozArchive)
- Fedora dev said (archive) (MozArchive) - *"I'm going to refrain from speculating or opining about this until I sync with the project's nominal legal assistance concerning impact"*. Prime suspect for cucking in the end.
- PopOS dev writes an entire essay to explain how the law sucks, then cucks anyway (archive) (MozArchive) - *"We are accustomed to adding operating system features to comply with laws. Accessibility features for ADA, and power efficiency settings for Energy Star regulations are two examples. We are a part of this world and we believe in the rule of law. We still hope these laws will be recognized for the folly they are and removed from the books or found unconstitutional."*
- Giant Debian thread planning the detailed ways of cuckery (archive) (MozArchive).

And if you want to say "oh, it's just Lolorado and Commiefornia!" then hold it, because obviously, the implementations will not care about where you are. In none of the cucking threads have I seen a mention that there will be two versions of OSes or apps - one cucked for

the people finding themselves in the unlucky regions, and another uncucked one for the rest. It would just be adding more effort for devs, maintainers, and so on. So they'll just bring it to everyone in the end. Also - knowing the recent obsession with inhibiting kids' online adventures - it's obvious Europe and everyone else will too jump into this soon. But hey, at least someone actually resisted properly (archive) (MozArchive).

And I realize that - in the form that it is now - this law is not accomplishing much (in terms of violating the users, I mean). The cucking OSes simply have to include an age bracket prompt, and the apps have to add maybe a few lines of code to "send a signal" for it. **The relevant data can be entirely faked**. But do you think the psychopaths will stop there? Of course not. This is just a Trojan horse to enable and enforce data collection. After the initial barrier is busted, they will be able to increase requirements in any way they want to. Face, iris scans, fingerprints, voice recognition, anything at all to "verify" you on the internet. And since the capabilities will be there already in all major OSes, not much will be possible to get done at that point.

Either way, this situation (once again...) shows very clearly that we can't rely on exclusively software means to stay free. Many fled to computers and the internet as their solace, since the physical world is so inadequate, but that option might be soon gone. In the end, nerds don't seem to have what it takes to resist in ways that truly matter. These would include (in this case) black market uncompromised OSes, likely spread physically through DVDs, USBs, and so on. Anonymous repos hosted on the darknets. But in the end we'll have to get even more physical than that. Own factories to produce hardware that is free of compromise, because they'll surely be trying to ban unapproved devices from going online soon. Obviously own ISPs so that such blocks can be prevented. And most importantly, controlling the legal system so that laws like this can be cut down before they blossom.

But what about decentralization?

Hiding or moving the problem. The "federated instances" always suffer from lack of activity, unreliability / short-livedness (hey, why aren't we all hosting our own shit? That's right...), and being subject to the whim of an internet stranger instead of a big corpo. Or take torrents. How many seeds does your favorite anime series have? How about something less popular, like video game soundtracks? People also get notices from their ISPs (VPN / TOR is just moving the problem again) if they didn't like their torrenting; some are apparently fined (archive). And of course, torrent sites still get taken down or compromised (archive) (MozArchive). Mesh networks? Yeah, like anyone's going to bother. Even if there theoretically was a decentralized solution worth shit, the governments might simply decide to kill off the whole Internet once they can't control people through it. Or install backdoors in the encryption algorithms or any one of the devices that are used for the meshnet. Again, our enemies have bigger resources / influence than us. Therefore, even decentralization would be temporary in the end - we will need their infrastructure eventually. In that case, we could also take control of something like YouTube or MEGA and keep their popularity and all the content, but change design / policies / TOS, so that users are guaranteed basic respect, privacy and freedom.

Services are not your friends

Yesterday a friend sent me this video, which explains how (in short) a VPN company bankrupted and got bought by another company, which then refused to honor the lifetime subscriptions of the customers of the original one. At the end, the author showed his wiki outlining the unethical practices of various companies; he pleaded for people to help fill it as well as suggested making a browser extension so that people are notified of corpo

transgressions anytime they go onto their sites. This is a great initiative but I fear it might not be enough. Why?

Because these are all **defensive movements** - we're always on the back foot, having to stay hypervigilant without any way to actually retaliate - just hope the opponent tires out. "Look, we found on this wiki that this company did X bad thing!". And what then? We run. We run to a company that's not listed on the wiki, hoping it lacks the skeletons in its closet. But, even if that's the case, it could become "bad" at any time. And then we run again. **The "free market" ideology is simply glorifying constant running**! And it should be obvious by now that it has failed. To hammer the point, let's try to find out what's required to run your own website:

Of course, you need to find a host. Since you don't want to reveal your "real" identity, you immediately dismiss all the ones that require such, and are left with only a few. If you want to pay in Monero and not shitcoins such as Bitcoin (archive) (MozArchive), some of them will be eliminated. If you want no arbitrary censorship, even more will be eliminated (archive) (MozArchive). After all that painstaking research, you finally find some service to settle on...or so you think, only to find out issues later. When I decided to move from Neocities to a VPS, Incognet seemed the "best" out of everything that was available back then. As it turned out, it was an illusion. Their portal was extremely slow and resource intensive, and kept logging me out every so often. But since I didn't have to enter it a lot, I could deal with it. However, since it was annoying to pay for my host every month, I had to eventually succumb to paying them in advance for a year or two, and letting it "renew itself". It becomes a problem when you don't want to use their service anymore, because (archive) (MozArchive) *“Crypto payments are non-refundable”*. So, their design goads you into paying in advance, but then you can't withdraw the money after you realize something bad about them, or they simply change policies - which has already happened:

> *Due to a changing legal landscape in the Netherlands, we prohibit the use of our services to make public any material from an IncogNET IP that you do not have permission to redistribute. This includes (but not limited to) hosting IPTV streams, sharing videos, pictures, music, ebooks or other media that you do not have permission to share, etc. This rule has always applied to our United States service locations, and is now being applied to our Netherlands location.*

Of course, they are not unique in this. Most hosts - or any services, actually - have a clause such as "we can change policies at any time", or "we can delete you at any time", or "we can sell at any time and your data will end up in the hands of our buyer", etc. When searching anonymous hosts I picked this "Evolution Host" from a list at random, and checked their ToS (archive) (MozArchive). And as expected, it says: *"Evolution Host reserves the right to change or alter our terms/policies at any time. It is the client's responsibility to check our terms regularly for any updates/changes"*. So, the "customer" pays in advance for a product, that can change at any time and kick him out at any time, without the possibility of refunds, and his only way of "resisting" is complaining to support... And what if the support system is also defective, like it is at Incognet, which doesn't even respond to E-mails? Their portal also went down for over a month at one point, so even posting support tickets wouldn't have worked. What if someone's server was about to expire during that span of time? They'd just lose it, without recourse. Even if you still had access, switching a host is actually a massive burden, so people might remain at their current one even if serious flaws have surfaced. **It is possible to pay for a service due to "reason X", then have no recourse while they do a 180 on it**. Isn't it obvious that the entire game is rigged heavily in favor of the "service"?

Think about it: why should an invention of civilization be allowed to be appropriated by a few (let's say airline) companies? Why should we not have a say into how they are run? An actual

say, and not running and hoping another company will fit our needs. Some people are required to fly for jobs, etc. And they shouldn't have to be dealing with research on which retard company (archive) (MozArchive) doesn't ban the unvaccinated (what if it's none?), for example. Unlimited property rights - the current pillar of civilization - are absolutely insane; and all this bullshit relies on them. Libertarians call it freedom but it is a fake freedom, one in which a couple big business owners pull their "customers" by leashes; pretty much a scam. And a wiki or even a browser extension is not enough to combat this problem. How many will even learn about the site? How many will download the extension? (most people do not use extensions AT ALL!).

I wish Louis Rossman luck in fighting the system - the same way I wished Ross Scott (who tried to "message his representatives" about consumer protection issues and learned the hard way that they don't care). But I very much doubt his initiative will suffice. I mean, think of how many things an average person needs just to lead a "regular" life. Shoes and other clothes, food, a fridge, a washing machine, cleaning products, a computer, an internet connection, probably a car or other means of traveling, furniture...and those are just the basics. What about supplements, medicine, games, cosmetics, and other things that are not strictly "essential"? All of those are potential minefields. **We clearly went wrong somewhere when wanting to take advantage of any invention of civilization requires "researching companies" who provide access to them**. Companies who don't really care about the product quality, or the environment, or customer dignity, or treatment of their employees - only the resources they can extract from you whatever the cost. And since they always dodge accountability, our only recourse in the current system is running. This needs to change. And it changes by...

What will save us?

...**Reclaiming the infrastructure from the forces of evil**. If I didn't make my point clear enough earlier, well, I will now. **Everything goes back to the physical**! We can't keep pretending that putting digital bandages over physical wounds works. The problem is inside the routers, the processors, the datacenters, the wires. The capitalist system that benefits from collecting data. And the legal system that allows and justifies abuses. We need our own factories, our own cities - that are designed with privacy and respect in mind. No more begging or running - we just change the relevant functionality directly. Imagine how many useless and / or malicious things could be eliminated, if only the actually affected people had control over them.

We are all cucks

We all connect through ISPs, having to sign contracts that might not have our best interests in mind, e.g banning hosting or WiFi sharing. Those ISPs might also collect data, share or sell it wherever, give it to the feds, inject ads, block protocols, censor "misinformation", or do literally anything else - and we cannot stop it. To produce our computers, we rely on corporations that integrate malicious stuff like Intel IME or Microsoft Pluton into the parts. Though we might use open systems for ourselves, Windows is still everywhere at institutions. And those open systems (e.g Linux) are increasingly being taken over by corporations, anyway. We rely on Twitter or Facebook for outreach, hoping they are not going to kick us out for "misinformation". And those companies are so big, that even national governments or political parties (archive) (MozArchive) are subservient to their whims. We rely on YouTube for hosting videos, and feel smart and cunning when we wear a condom like Invidious, but the corporation upstream can break the condom at any time. And so we toil fixing the frontends (archive) (MozArchive) every time our masters decide to ruin something. Even our FOSS is hosted on a service ran by the biggest anti-FOSS company, funnily enough. We rely on donation platforms

like PayPal or GoFundMe that can block our funds (archive) (MozArchive) if they decide we're undesirable. We hunt down ad networks to add to our filter lists, only to be foiled again and again by the advertisers and trackers. We think our darknets will save us, when they all still go through the enemy's networks and can be easily blocked. **We're fucking cucks**! I mean, look at this guy and tell me he's not totally embarrassing. Or look at all the people complaining about YouTube's removal of the dislike count.

You can uncuck yourself individually up to the level of maybe 80% if you're really skilled / determined. But it's going to take a lot of sacrifice and is never going to reach 100%, anyway. It is also going to become increasingly harder as time goes on and every newly invented technology also becomes apart of the same slavery scheme. I am so tired of playing the whack-a-mole game with evil. Let's tackle it at its cores. What we are doing today are band-aid fixes over stuff that exists solely because evil people are currently in charge. Yet we are all just deluding ourselves through the band-aids. How can you simply install an adblocker and forget about what it represents? The only reason ads exist is because they earn profit for the companies that display them. Yet people happily swallow the capitalist bedrock of society while offloading its costs onto the (most) people who don't install an adblocker. This is of course all going to come crashing down soon, for example when grass (archive) (MozArchive) or sky (archive) (MozArchive) ads become more common. The same applies to closed source software - organizations like the FSF whine and whine about the evils of it, but love the profit motive (archive) (MozArchive) that births it - or they even welcome the corporations into FOSS and pretend they won't have a negative effect (archive) (MozArchive) there. See? It's cuckery all the way down even when "solutions" are involved. How about cryptocurrency? You can barely buy anything for it and are still probably going to need a bank account just to live. And in many places, it is very inconvenient to use crypto with how hard it is to get it

anonymously (the crucial advantage). It is all also dependent on the infrastructure of the Internet and electricity. As I said before, we need to set up a society with the values we care about (privacy, anonymity, freedom of speech, and others) baked in, instead of put on top as afterthoughts. It is not **just** about the profit motive - that's just one example. Power and control are motivations in themselves for some people. And so you have the spying, censorship, etc for the purpose of keeping power. So we have to move the scale of power towards our side, but I feel like everything in this society is set up to prevent that. For example, people believe things like:

- The law is the law, you gotta follow it. Vote better if you don't like it!
- A private company can do whatever it wants without consequence. Vote with your feet / dollar!
- Property rights are sacred. Don't you dare deface those ads or destroy those CCTV cameras!
- Profit motive is amazing, rewards "merit" and "creates innovation". The alternative is communism, and that's bad and killed gorillions of people!

The powerful spread the memes that keep the power in their hands, while the plebs repeat them and believe them as if they themselves benefitted from those ideas. If that isn't the ultimate cuckery, I don't know what is. But it is also cucked to think we can solve all our problems by typing away at our keyboards while ceding all physical territory to the forces of the dark.

Society needs sane defaults

We can't expect your secretary or plumber to become an expert in technology and fish out

Monero, self-hosting and mesh devices from the sea of deadly sharks. Just like we shouldn't need to become experts in nutrition just so we can pick out the few foods that won't make us sick. But the theme of this report is tech, so that is what we will stick to. Anyway, the peak of ethics in society will be reached only when a regular person can just jump into the popular choices and be rewarded with ease of use, anonymity, privacy, freedom of speech, good functionality, etc. When the Windowses, YouTubes, Discords, Facebooks, bank accounts or their future equivalents, ISPs are not trying to abuse us at all times and are at least mildly ethical. Imagine all the wasted manpower on those now! Imagine all the infrastructure that could be repurposed for good, while we have to do with breadcrumbs... These institutions need to either be regulated to hell, reformed by insiders, or burned down and replaced with something better. How exactly that is going to happen, I have no idea. But the defaults need to become sane for our society to be sane, too. Maybe then our current band-aids of darknets and crypto won't be so necessary. Of course, I'm not delusional enough to think that a "one product to rule them all" can be created, so there will still be a place for enthusiasts to roll their own setups. But at least the basics should be able to be ensured for the normies. And so, can we answer the title's question of whether *“Avoiding The Botnet”* is *“impossible”*? Well, with the current mindset this would be an empathic YES. But with proper fundamental modifications to how the world works, we can in fact bury *“The Botnet”*. And let's end on this good note.

Back to the front page