E-mail providers - which one to choose?

- OpenMailBox (DEAD) -
- Runbox -
- Mailfence -
- Safe-Mail (safe-mail.nl) -
- Neomailbox -
- Mailbox.org -
- Secmail.pro -
- CTemplar (DEAD) -
- KolabNow -
- Teknik -
- Tutanota -
- Autistici -
- StartMail -
- Dismail -
- Migadu -
- Cock.li -
- Paranoid.email -
- Cotse -
- CounterMail -
- Fedora Email -
- Posteo -
- Morke -
- Disroot -
- Elude -
- RiseUp -

Introduction

E-mail is the well known communication system brought to the digital world. It's useful mainly for signing up for stuff, but also to receive and send messages to other people. To use it, you need a provider (or you can host your own, but we won't cover that here) and either a web browser or a mail client (the superior option). Various providers have their pros and cons, and choosing one can seem overwhelming - especially with the amount of hype many of them are throwing around. I'll try to make this really simple. **The most important features a service should have are mail client and anonymization support**. If a provider lacks either one, they are disqualified, in my opinion. There are many reasons why mail client support is so important. First of all, you can **choose the program you like**, and make it fit within your workflow, instead of depending on whatever special snowflake JavaScript your provider comes up with. Your mail client software will always stay the same, while a webmail service can change their JavaScript at any time - including to make it malicious or incompatible with your web browser. **Standardized protocols allow the downloading of mail to your computer**; they **keep the control in your hands**, instead of a big corpo. A good mail client will surely outcompete webmail in terms of features. It also takes the weight off a web browser, which should really focus on just browsing the web (unix philosophy - one application per task). But perhaps the most important issue is that mail clients **support established encryption** in PGP; while webmail-only providers sometimes don't - and even if they do, **it is not as secure** when used that way.

The other feature - anonymization support - should be obvious. You don't want the stuff you do on the Internet to connect to your real identity, lest it be used against you sometime in the future. This means you need to be able to sign up with a VPN or the TOR network; as well as avoid revealing data such as real name or phone number. There are a few other things you might want to look for, but these two are the fundamentals that can't be replaced. An alias feature allows you to have many unconnected identities (for example, one for "professional" work, and another for sperging out about vidya or anime) within the same account. A good privacy policy that limits the amount of collected information - I mean, we don't tolerate spyware browsers, neither should we spyware providers. Then comes the price - free is the best; **a paid provider better support Bitcoin** if they want the highest grade. A mild ToS which won't ban you for homophobia or some other victimization issue of the day (still, a provider should not be reading your mail, and you should be encrypting yours, if possible). Most of the other stuff that services use to advertise themselves is pretty much hype; it's a jungle out there, and providers will try anything to get ahead of the competition. Keep the fundamentals in mind while reading this report (hint: providers are sorted from worst to best)!

List of providers

Hushmail

> *Everyone is entitled to their email privacy. Take back control of your data and experience a clean inbox with no advertising.*

Okay, I'm in! Just give me a minute to check if the evidence supports your claims...

> *When you visit our website we may collect information about you, including your browser type, operating system and the Internet Protocol ("IP") address of your computer. We use this information to facilitate your use of the website,* ***gather market information*** *and prevent abuse of our services.*

No thanks. But wait, that's only the website - I could possibly deal with that if the actual mail service was private. But is it?

> *We take steps where possible to limit the personal information we collect.*

Wow, thanks! So let's see just how limited those "limits" are:

> *As part of the account creation process your IP address will be recorded. We may request that you provide other information, such as a* ***phone number****, as well. We use this information to analyze market trends, gather broad demographic information [...]*

Asking for my phone number is very "limited" indeed. And the market trends shit rears its ugly head again.

> *nformation we record may include [...] account usernames, sender and recipient email addresses, file names of attachments, subjects of emails, URLs in the bodies of unencrypted email, and any other information that we deem necessary to record for the purposes of maintaining the system and preventing abuse.*

So you're even snooping on the links in my messages! And *"any other information"* is an admission that they could possibly collect everything they imagine. But why pretend it's about

“preventing abuse”? Just say you're in the business of gathering information.

> *We store sales, marketing, and customer care information with third-parties that support these business processes, which means that information such as your name, email address, phone number, and company name, as well as the history of communications related specifically to the sales or customer care process, may be stored there.*

And now my name and phone number is being sent to whoever the fuck. **Could this get any worse?**

> *The records we keep of your activities are permanently deleted after approximately 18 months. Records that are stored for statistical purposes may be kept indefinitely.*

...yes, it could in fact get worse. And that's not even the entirety of it (I don't want to write a book here!) - check out their privacy policy (archive) (MozArchive) if you want to torture yourself further.

I forgot to mention that Hushmail actually **wants money for all this abuse!** And it doesn't even support mail clients. Taking all that into account, this is without a doubt **the worst choice on this whole list**. And they have the audacity to claim stuff like this:

> *Hushmail has been providing secure, private and encrypted webmail solutions since 1999. Here is why our customers trust our experience in the field.*

Yeah sure - very trustworthy you are! **UPDATE February 2023**: now they are also Cloudflared. Truly climbing mountains in their quest to be the worst possible E-mail provider.

FastMail

UPDATE February 2023: Fighting hard for the first spot, **FastMail is also now Cloudflared.**

This is another one of the paid providers which are also absolutely terrible from a privacy standpoint. From their privacy policy (archive) (MozArchive):

> *If you register to use, or use, one of our websites or services [...] personal information that may be collected directly from you includes name, billing address, mobile phone number, organisation name, your own domain name, IP address, browser user-agent and billing details*

Name, phone number, address. You're off to a fast start towards privacy hell, FastMail.

> *We process mail sent and received from your account to block spam and fraud.*

The private FastMail **scans your mail**.

> *We also store information from your address book, calendar, notes and files on our servers.*

Is there anything you guys **don't** store?

> *We also collect the email content you create, upload, or receive from others*

Guess not - even other people aren't safe from FastMail's prying eyes.

> *Each time you connect to our service, we log your IP address, your client identifier (browser or mail client information) and your username. If you send mail, we also log the email address you're using to send mail and the email address you're sending to. If you* ***take action on mail*** *in your mailbox, we also log the activities taken.*

So literally your every move is being tracked and logged. And now for some humor - look at how they justify themselves:

> *This is necessary for providing proof of delivery and fraud analysis.*

Sure. I wonder why almost **no other provider on this list is doing so**, then? Now check this admission (from section *"How do we use the personal information we collect from you?"*):

> *conduct analytics and measurement to understand how our services are used;*

Oh, so it was about **analytics** all along, instead of *"fraud analysis"* or some other bullshit excuse. And for something even more damning (from section *"Sharing personal information with others"*):

> *We may share your personal information [...] with third parties who help manage our business and deliver services [...] Some of these providers use "cloud based" IT applications or systems, which means that your Personal Information will be hosted on their servers*

And now all the stuff I've talked about will be put on some third party servers.

> *We may use your name and email address to send direct marketing communications to you and let you know more about our services or related services that we believe will be of interest to you*

You will also be flooded with directed advertisements. But how does FastMail know what *"will be of interest to you"*? Of course, it's because of all that collected data - which, remember - **includes your mail content**! Later they claim that they don't profile you to send targeted advertisements, but that seems to contradict the above - and we should **always assume the worst**. FastMail also uses the Matomo tracking service, which was described in detail in ProtonMail's section. Anyway, that's quite a lot of data collected - but how long does it stay around?

> *Where we log information related to your IP address, we retain this information for approximately 90 days.*
>
> *Where you request that we delete your account from our system, we will immediately lock the account and archive the information, then delete it from our severs within approximately 7 days from the date of your request.*

Not bad, I guess. I mean, some other providers take a year or more...But wait:

> *However, in specific limited circumstances we may store your personal information for longer periods of time*

Ha! So the 7 days figure was just for show. Let me quote some related information from another section (archive) (MozArchive):

> *After an account is terminated, data and backups are purged within a timeframe of between 37 days to 1 year after closure*

So you **do** take a year after all. And you **fucking lied** straight to our faces with the 7 day thing. This seems more and more like some entry-level trolling...Can we say anything at all positive about FastMail in light of the information presented? I guess this:

> *Providing secure end-to-end encryption via webmail is impossible. There are basically two options, both flawed:*

That's right - it's the same thing I've been speaking about. So at least they don't pretend to have some super-duper in-browser encryption. And maybe another thing:

> *We won't release any data without the required legal authorisation from an Australian court. As an Australian company, we do not respond to US court orders.*

But remember that some of your data will be stored on third party servers in other countries, which might have some different ideas...All in all, I struggle to provide a reason to use this one at all. The amount of stored data is simply massive (and I didn't even cover all of it), it's shared with third parties and used for sending advertisements - and you have to pay for all that.

Skiff

UPDATE February 2024: bought by (archive) (MozArchive) some shady corporation. And killing their mail in 6 months:

we will be closing down Skiff's product suite after a 6-month sunset period

You can now also set up a forwarding address to redirect mail to any other provider.

It was always a project based solely on profit. The profit dried up, and the scammers ran, hoping for their one last squeeze of profit, which I guess they received out of this acquisition. Don't forget that according to their old ToS, **selling your data was absolutely on the menu** in a merge situation. Anyway, here is the old review:

Hey, it's been a long time - and my hands are itching for some action. Fortunately I have my chainsaw right here, ready to cut down another shitty provider ^_^. First of all, **Skiff is Cloudflared** - even the signup page - meaning CF steals your password. This should completely disqualify it already, but I'm Diggy and the job has only begun. The registration process requires malicious hCaptcha, and I'm not going to solve that shit. If you're wondering what hCaptcha is - it's just reCaptcha sans Google. It pretends to be private, but isn't (archive) (MozArchive):

Other information collected from End-Users as part of the Service to that is required to determine whether they are human, such as mouse movements, scroll position, keypress events, touch events, and gyroscope / accelerometer information as applicable.

Your captcha solutions will also be fed to an AI and shared with the website on which hCaptcha is embedded:

To provide a market for Labeled Data. Our Service enables high volume data labeling and human review for machine learning systems as a service to website owners and

> *companies who need help getting their data labeled. To that end, we disclose Labeled Data to our Customers interested in acquiring Labeled Data.*

You're a lab rat, *"labeling"* data for *"machine learning systems"*. How comfortable does that make you feel? And surely, those *"machine learning systems"* will be used against us down the road with police bots and such - who will now be able to recognize objects because **you've told them what they are**. By the way, hCaptcha itself **is Cloudflared**, so they also get all this data. But let's go back to Skiff.

If you still want to register for Skiff despite this abuse, realize that **the registration page does not work properly in Pale Moon** (nor many other pages; I cannot even read the help page). The site starts executing some heavy JS, fan can be heard working in overdrive...but still, nothing displays. Not even through the Wayback Machine so it's not even the CF doing that; the code is just incompatible - Skiff obviously wants to give up the Web to Google and its minions (like Mozilla). But okay - you will say; I will just submit to overlord Google and use Chrome to sign up. What are you getting?

A service that **does not support mail clients**! As if Skiff did not earn enough red cards already, here we have yet another reason to kick it off the field for the people that didn't get the memo yet...(read the intro to see why mail clients are so important). The lack of support for mail clients also allows Skiff to keep certain features hostage (such as the amount of *"Folders and labels"*) that would be freely available in a mail client. This way they get you to go for the paid plans. But even the paid plans are worse than the free ones of mail-client-supporting providers, so what's the point? They also shill *"End-to-end encryption"*, which works the way you'd guess - only between Skiff victims. Recall how JavaScript-dependent E2E could be broken at any time by the provider by substituting compromised JS. But here it's even worse, because the

Cloudflare MitM could do it themselves. Skiff also offers a Drive, Calendar, and some collaboration tool available - but here we're only covering the E-mail. Anyway, for more dirt on Skiff let's check out their ToS page (archive):

> *3.4. Use of Customer Materials. In consideration of your use of the Services, you hereby grant to Skiff, its parents, subsidiaries, affiliates, licensees, designees, and successors and assigns a limited, non-exclusive right to use, copy, distribute and display Customer Materials*

"Customer Materials" = all the data that's received from you. Skiff claims ownership of it and will throw it around unknown (to you) shady entities. How about their privacy page (archive)?

> *Skiff's highest priority is to safeguard the privacy of the users on our platform. While you are on our platform, we collect only a minimal amount of data needed to provide you with our services.*

The usual privacy posturing. But is it justified? Spoiler - lolno:

> *Automatic Data Collection. In order to protect you and our platform from malicious activity and to prevent fraud, we may collect certain information automatically when you use our Services, such as your Internet protocol (IP) address (temporarily), user settings, and Skiff-provided authentication cookies. We may also temporarily collect information regarding your use of our Services, such as pages that you visit before, during and after using our Services, the frequency and duration of your activities, and other information about how you use our Services.*

So they spy on you pretty specifically, tracking your movements across the site and with timestamps attached - and even **outside Skiff itself**. It is clear they want to lay their hands on as much as they can - and forever, too:

> *We store the personal information we collect as described in this Privacy Policy for as long as you use our Services or as necessary to fulfill the purpose(s) for which it was collected, provide our Services, resolve disputes, establish legal defenses, conduct audits, pursue legitimate business purposes, enforce our agreements, and comply with applicable laws.*

You never get told the actual duration (in amount of days, etc - not even a range) - so the *"temporary"* storage appears to be a **lie**. Skiff will also give away all your data to a would-be buyer (I guess that's what the forever storage is for):

> *If we are involved in a merger, acquisition, financing due diligence, reorganization, bankruptcy, receivership, purchase or sale of assets, or transition of service to another provider, your information may be sold or transferred as part of such a transaction*

They also do targeted ads and location tracking:

> *You can use your mobile device settings to limit use of the identifier(s) associated with your device for **interest-based advertising purposes and for location tracking**.*

You can graciously delete / block the cookies responsible for the tracking (apparently; I can't sign up so I can't audit this more specifically). But then...

However, if you adjust your preferences, our Services may not work properly.

Hahaha. **You will watch our ads and you will be happy**. Anyway, this service appears to be completely useless; I cannot even justify it over something like Gmail or Outlook - which is quite an achievement for Skiff. You'd think that with me being inside this provider review "business" for so long, there would come a time where I could say I've seen everything - but it doesn't appear to be approaching yet. And if I was able to actually sign up and enter this swamp I'd probably be able to discover even more bullshit, but I'm not solving that shitty captcha, so this will have to suffice (hey, I already feel dirty about having to run ug-c just to view their broken pages).

Outlook

Since Google got one, then surely Microsoft must be the next in line for the chopping block. It's actually really similar to Gmail, but maybe **even worse**. Sign-up process is a mirror image of Google's, except you need to enable more stuff in uMatrix so that it works. Otherwise, it requires your real name and phone confirmation - which I (obviously) didn't bother with, so I don't know what comes further. As with Gmail, you can't sign up for just the E-mail, but instead get a Microsoft account containing access to all their services. Let's analyze their privacy policy (MozArchive) now (better have some painkillers ready, because **it hurts**):

> *Data about your device, your device configuration, and nearby networks. For example, data about the operating systems and other software installed on your device, including product keys. In addition, IP address, device identifiers (such as the IMEI number for phones), regional and language settings, and information about WLAN access points near*

your device.

It's not enough for them to know how you're using their services - Microsoft will also snoop on everything else you're doing with your machine. Ugh.

> *Data about your interests and favorites, such as the sports teams you follow, the programming languages you prefer, the stocks you track, or cities you add to track things like weather or traffic. In addition to those you explicitly provide, your interests and favorites can also be inferred or derived from other data we collect.*

Not sure how applicable the above is to E-mail specifically - but it clearly shows the attitude of Microsoft towards your privacy - which is a complete disregard for it.

> *Data about your contacts and relationships if you use a product to share information with others, manage contacts, communicate with others, or improve your productivity.*
>
> *Information about your relationships and interactions between you, other people, and organizations, such as types of engagement (e.g., likes, dislikes, events, etc.) related to people and organizations.*
>
> *Data generated through your use of Microsoft's communications services. Traffic data indicates with whom you have communicated and when your communications occurred*

Now **these are** surely relevant to E-mail. Not only does Microsoft keep your contact list, but also when you have written them. What about the duration of data storage? Unlike Google, Microsoft does graciously tell us something about it:

> *when your Deleted Items folder is emptied, those emptied items remain in our system for up to 30 days before final deletion*

So, we know that - when we delete an E-mail - it's gone in 30 days at most. This sucks, but at least we get told about it - which many allegedly private providers can't manage to muster. As for the other data, we're unfortunately left with vague statements such as:

> *Microsoft retains personal data for as long as necessary to provide the products and fulfill the transactions you have requested, or for other legitimate purposes such as complying with our legal obligations, resolving disputes, and enforcing our agreements.*

Realistically - considering the avalanche of various anti-privacy and anti-user stuff in their policy - we should assume the other data is stored for much longer than the actual mail content (you'd think they'd mention the duration if it was something they could have bragged about). Okay, there's just one more transgression of note that I want to cover:

> *To build, train, and improve the accuracy of our automated methods of processing (including AI), we manually review some of the predictions and inferences produced by the automated methods against the underlying data from which the predictions and inferences were made.*

That's right - **Microsoft uses your data to train their AI**. The same crap Google has been pulling for years with their ReCaptcha. If you were considering Outlook as your E-mail provider (why?), this alone should drive you away from it. The ToS (MozArchive) also makes SJWs look like freedom lovers by comparison. Same as with Gmail, Outlook does support mail clients and is free - which are the only advantages of the service.

Gmail

Fuck it, I'll give it a proper review, because why not? It's not even the worst provider out there, if you can believe it. It does support mail clients, for one - so it automatically has an advantage over many of the ones advertising privacy and user respect that are webmail-only. My **VPN was not blocked**, though it did ask for my real name (which you can fake) as well as **requiring phone confirmation** - which I ended up choking on.

Unfortunately - as if it wasn't obvious - **mail client support is the only positive Gmail has**. And even that seems hollow when you realize that - in order to use Gmail with a third party client - you need to either have OAuth2 (web browser dependency), or set up an "App Password" in your Google Account, which requires you to give your phone number to Google and then activate 2FA in order to be able to create an "App Password". Another "benefit" of Gmail is that it's free - but you pay with giving up an amount of data (archive) (MozArchive) which other providers can only dream of matching. For example:

> *unique identifiers, browser type and settings, device type and settings, operating system, mobile network information including operator name and phone number and application version number. We also collect information about the interaction of your apps, browsers and devices with our services, including IP address, crash reports, system activity, and the date, time and referrer URL of your request.*
>
> *We use various technologies to collect and store information, including cookies, pixel tags, local storage, such as browser web storage or application data caches, databases and server logs.*

There is much more. It's not an exaggeration to state that **every step you take, every move you make** while using Google is stored and analyzed (and the duration is not stated, as far as I can see - so assume it's **forever**). What makes it worse is that you can't sign up just for Gmail, but need a Google account for every one of their services. So, if you're logged in (because you're using their webmail, for example), then they can also track you all over YouTube, etc. and mix up all the information to make a profile. Google is also a PRISM member, so your stuff is likely ending up grabbed by law enforcement (they've shared location data (archive) (MozArchive) with them before). And, using Google's services means you enable all their unethical practices (such as shoving ReCaptcha into our faces, heavy censorship on their search engine, widespread tracking and ads, their monopoly on browsers, etc). Other providers - even those of the spying sort - pretty much limit themselves to mail; they don't have the worldwide influence on so many things as Google does. So, **you should specifically avoid Gmail** just to inhibit their quest for world domination (did you know they can even lock you out of your house (archive) (MozArchive)?) - even if they're not the worst provider out there.

Gandi

I wasn't supposed to review any more trash providers but this one stood out and someone requested it, as well. I'll be quick here, I promise. **You need to get a domain with these guys before registering for their E-mail**. The domain registration process needs an account with your real name, phone number, E-mail address and physical address. If that wasn't enough torture: to pay with cryptocurrency, you need to register for the third party payment provider BitPay - which is Cloudflared, requires solving reCaptcha, and providing them **a fucking ID document**! Holy shit. Are you a masochist? Then Gandi is the perfect provider for you! And yet, they have the audacity to advertise themselves as having *“no bullshit”*...

VFEmail

UPDATE May 2022: requires reCaptcha again, but allows bypassing it by *“upgrading”* your account, whatever that means (probably paying). Still asks for your real name; registration also fails on Pale Moon. Everything else is as shit as it was when I wrote the first report, except **the site is now behind the evil** Cloudflare**.** Mail clients are supported, but auto-configure doesn't seem to work. Accepts signing up from a VPN, and that's where the positives end...A lot of suspicious things in the user agreement; going over all of them would take a year, so I will discuss only the most important ones:

> *[...] VFEmail.net can terminate and/or change and/or modify your account [...]*

Wait, *“modify my account”*? What the fuck? This can literally mean anything, including rewriting your mail, deleting contacts, or changing the password. Suspicious as fuck!

> *[...] VFEmail.net or its designee may disclose information to third parties about User and User's use of the Service [...]*

Great! Prepare yourself for your privacy being ripped away and thrown around to advertisers and trackers.

> *User acknowledges and agrees that content, including but not limited to text, software, music, sound, photographs, graphics, video, or other material contained in sponsor advertisements or information presented to User through the Service or advertisers is protected by copyrights, trademarks, service marks, patents, or other proprietary rights and laws.*

So you will be sent advertisements and can't even show them to anyone. By the way, I've confirmed **they add ads to your mail**. Whenever you send anything from the free VFEmail account, your recipient gets this:

> *This free account was provided by VFEmail.net - report spam to abuse@vfemail.net ONLY AT VFEmail! - Use our Metadata Mitigator to keep your email out of the NSA's hands! $24.95 ONETIME Lifetime accounts with Privacy Features! 15GB disk! No bandwidth quotas! Commercial and Bulk Mail Options!*

Funny how they claim to protect you from the NSA when they are Cloudflared (a US company) and have no real privacy policy. With a free account, you don't even get SSL encryption on your mail. So it is sent around in plaintext, completely visible to your ISP for example. Now what if you've paid? You get SSL (congrats for being the only provider out there who doesn't provide that for free), aliases, no ads and unlimited bandwidth - but **are still in the dark** as to the privacy and still subject to the shitty ToS. And to lighten up the mood...

> *If you do recieve mail between your last POP and the snapshot at 12am, it will exist on backup for a week - unless it's on Saturday night, then it's a year.*

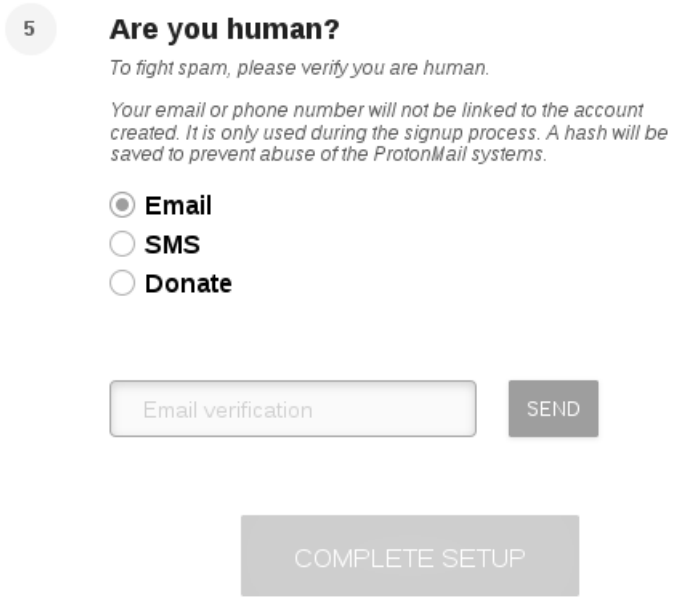
WTF? These guys must be trolling around here. Your mail is stored in a backup for a week...except on Saturdays! How random.

As for other data, you don't get told what gets stored and for how long. If you still didn't get the memo - **get away from this crap!** Honestly, it looks as if some jokers just slapped all the anti-user things they could think of, advertised themselves with bullshit like the *“Metadata Mitigator™”* - for which of course you have to pay - and went around their merry way while

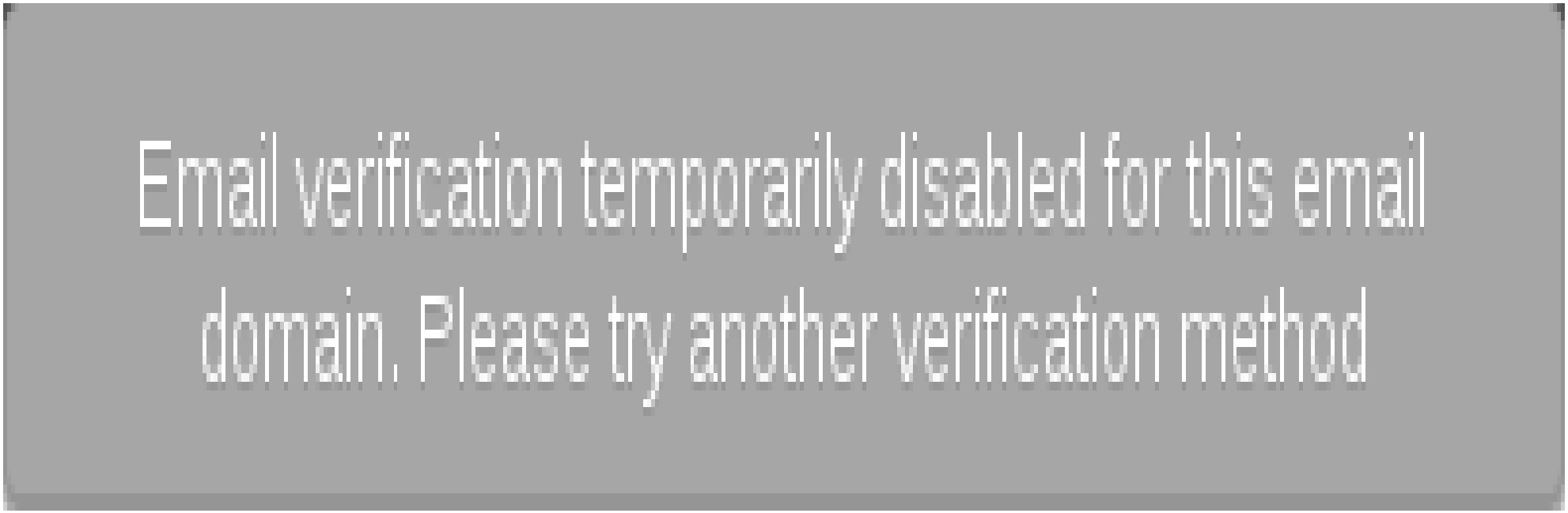
raking in the cash. This might be worse than Gmail, which is more honest in regards to their (lack of) privacy and provides all its features for free.

ProtonMail

The most popular "private" E-mail provider, and often the first choice of a person getting away from the three giants. But does that mean it is in fact quality? The site is filled by beautiful **black screen without JavaScript enabled**. But assuming you got past that hurdle, let's consider the sign-up process - if you're signing up through TOR or a VPN, ProtonMail **requires SMS confirmation**:



And if you try to receive confirmation through a RiseUp E-mail, it says this:



So, SMS is the only option (unless you want to donate, which would reveal your personal information of course); therefore their claim that *"ProtonMail does not require any personally identifiable information to register"* is a **shameless lie**. Proton later included the option to solve a hCaptcha (used to be reCaptcha) for confirmation; however, **the option disappears while using a VPN**. They must really want that damn phone number if you are using anonymizers! And the claim that you can sign up without personal data is still false.

The way their "end to end" encryption works is by **generating the encryption keys while you sign up** - using your already existing keys is not allowed and ProtonMail must store the generated private key (archive) (MozArchive) for PGP to work. Since the whole encryption process is done by JavaScript in the browser, **nothing prevents them from sending you backdoored JS**; the encrypted messages can also only be sent to other ProtonMail users, unless using the paid account (update: actually, a friend has told me that the latter isn't true anymore, though you have to upload the recipients' public PGP keys to ProtonMail if you want to use

them). According to researchers, ProtonMail's encryption contains serious shortcomings. At the end of this report, I also link to an article detailing the issues with in-browser encryption in general. Mail clients are not supported except, again, through a paid feature called *"Protonmail Bridge"*.

But let's move past the fluff and see which data does ProtonMail actually store and for how long. Quoting from their privacy policy (archive) (MozArchive):

> *We employ a local installation of Matomo, an open source analytics tool. Analytics are anonymized whenever possible and stored locally (and not on the cloud).*

So when you visit their website, this Matomo spies on you. But what data does it actually collect? From Matomo's website (archive) (MozArchive):

> *All standard statistics reports: top keywords and search engines, websites, social media websites, top page URLs, page titles, user countries, providers, operating system, browser marketshare, screen resolution, desktop VS mobile, engagement (time on site, pages per visit, repeated visits), top campaigns, custom variables, top entry/exit pages, downloaded files, and many more, classified into four main analytics report categories – Visitors, Actions, Referrers, Goals/Ecommerce (30+ reports)*

So that's the website. What about the e-mail service?

> *we have access to the following email metadata: sender and recipient email addresses, the IP address incoming messages originated from, message subject, and message sent and received times. [...] We also have access to the following records of account activity:*

> *number of messages sent, amount of storage space used, total number of messages, last login time.*

Great, even more metadata than Tutanota (if you trust Tutanota's claims that they collect as little metadata as they say they do). And then there's this gem:

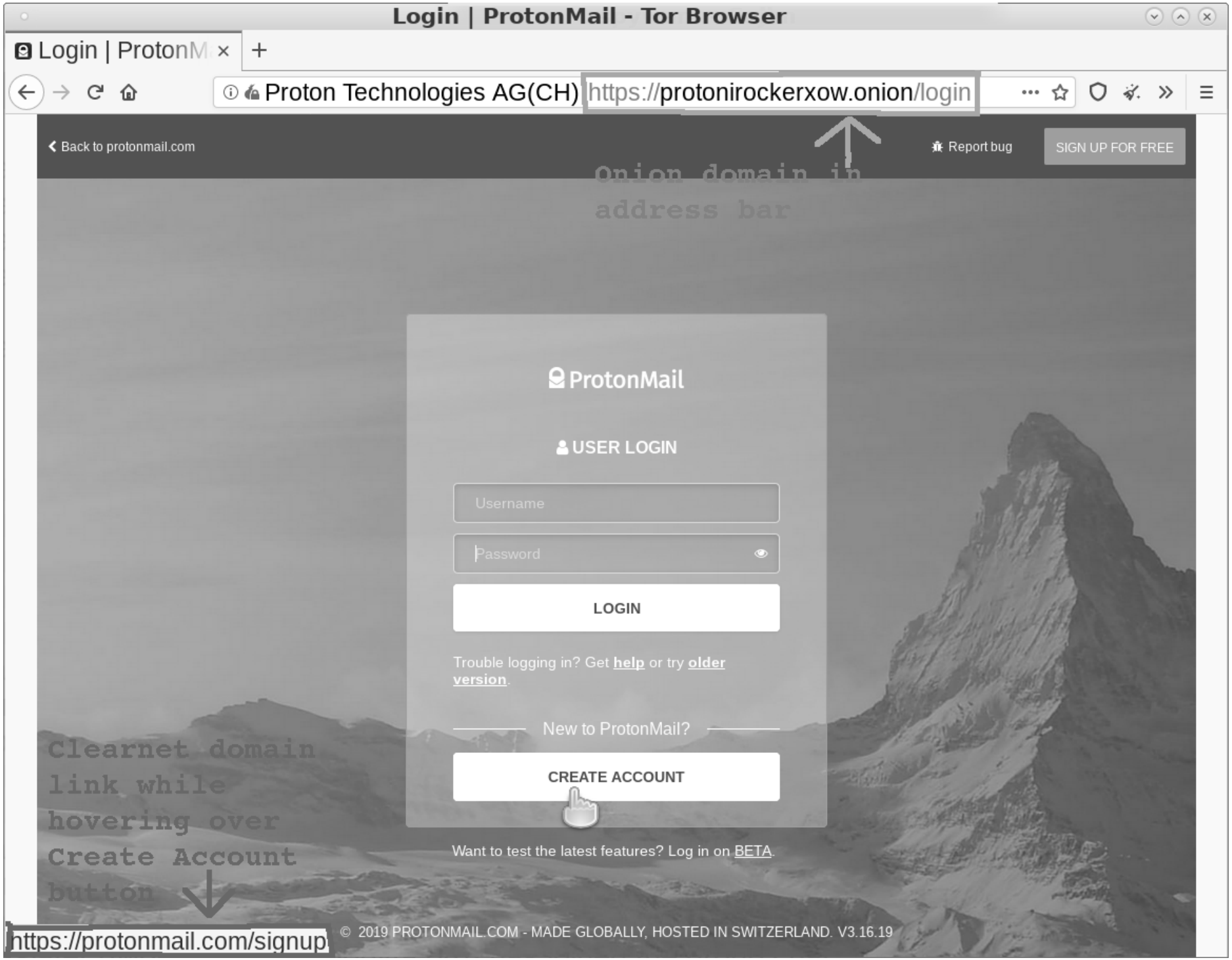
> *When a ProtonMail account is closed, data is immediately deleted from production servers.* ***Active accounts will have data retained indefinitely.*** *Deleted emails are also permanently deleted from production servers. Deleted data may be retained in our backups for up to 14 days.*

Read that again! Indefinite retention of data by the "private" ProtonMail! And 14 days for deleted data - enough for "them" to get you. At least there's disk encryption...UPDATE August 28; a direct admission they **do store IP logs forever** in certain cases - *"and your IP address may be retained permanently if you are engaged in activities that breach our terms and conditions"*. Their TOS says this: *"You agree to not use this Service for any unlawful or prohibited activities. You also agree to not disrupt the ProtonMail networks and servers"*, which can cover pretty much anything.

UPDATE June 2022: their new privacy policy (archive) (MozArchive) (which, by the way, now doesn't display without JavaScript) is kind of different, they deleted some of the offending stuff. Doesn't mean they are not doing it anymore, since they already have proven to violate the user many times.

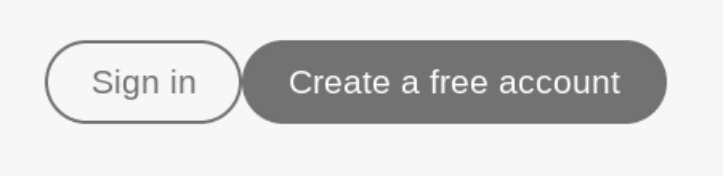
If you read their transparency report (archive) (MozArchive), you will see quite a lot of requests for their data from governments all around the world. ProtonMail pretends to "require

a Swiss court order" to cooperate - but you see that they often do that before receiving it - so don't expect that to protect you. One particularly egregious example is from May 2018, where they **disabled an account because of terrorist allegiances** - and we all know that's not just a convenient excuse these days, right? The new transparency report (MozArchive) shows they've complied with **336 government data requests** in 2018 alone - including 76 foreign ones. Oh, and since August 28, they **finally admit to direct surveillance** - *“In addition to the items listed in our privacy policy, in extreme criminal cases, ProtonMail may also be obligated to monitor the IP addresses which are being used to access the ProtonMail accounts which are engaged in criminal activities”*. And you will never be told you're being watched. So, what we have here is a provider that does not support mail clients, requires personal info to sign up while claiming otherwise, spies on you on their website, stores your e-mail metadata (and IP in certain cases) forever and immediately gives it up whenever government knocks on the door and shouts "terrorism!". Its encryption is also lacking according to researchers, and cannot be used for non-ProtonMail accounts without paying. And then - after all that - it claims to be a champion of privacy...As we can see, ProtonMail **is found out to be a paper tiger** when examined deeper. It does have an onion domain, but guess what - when you try to sign up through it, you are **redirected to the clearnet with no indicators** unless you happen to look at the address bar. This behavior is something I'd expect from **a honeypot** - you get lured with the added security of the onion domain, and then it's pulled away like the carrot on a stick. Avoid!

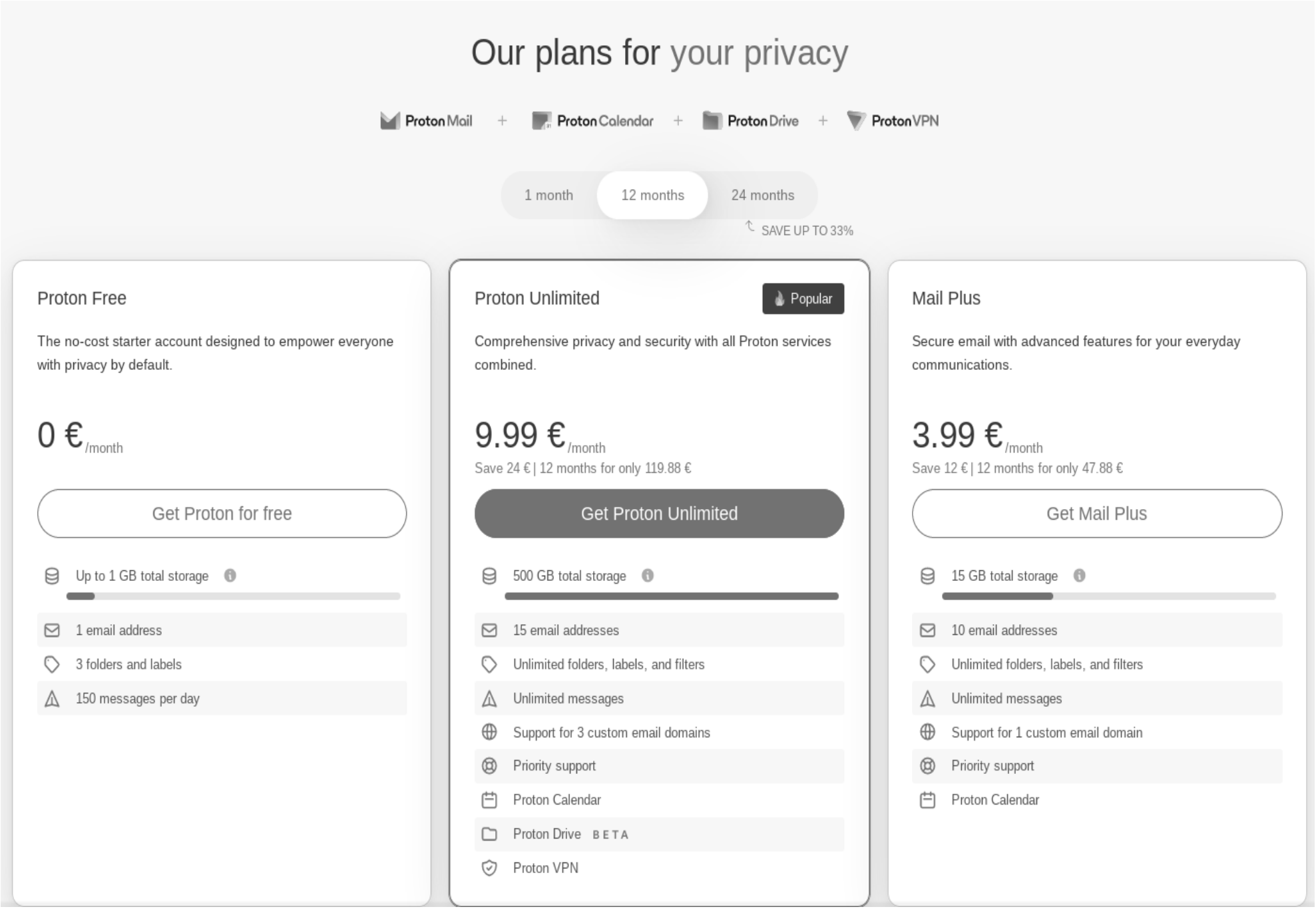

Login | ProtonMail - Tor Browser
Login | ProtonM
Proton Technologies AG(CH)
https://protonirockerxow.onion/login
Back to protonmail.com
Report bug
SIGN UP FOR FREE
Onion domain in address bar
ProtonMail
USER LOGIN
Username
Password
LOGIN
Trouble logging in? Get help or try older version.
New to ProtonMail?
CREATE ACCOUNT
Want to test the latest features? Log in on BETA.
Clearnet domain link while hovering over Create Account button
https://protonmail.com/signup
© 2019 PROTONMAIL.COM - MADE GLOBALLY, HOSTED IN SWITZERLAND. V3.16.19

UPDATE: this is no longer valid. But I'm leaving it up to show that these frauds do not care about security at all. And they still have OTHER clearnet redirects up! Even this one took them way too long to fix it. And they seemingly did it ONLY because I trashed them for it. Otherwise, you'd keep being violated by the malicious redirect, since ProtonFail still shows no indication of caring about the user at all.

UPDATE May 2022: the new interface contains dark patterns! Look:



This button appears on the index page. And when you click it, instead of a creation screen for the free account that you were promised, you see this:



Everything on this screen is trying to get you to buy the most expensive plan (even though *"Mail Plus"* provides pretty much the same features if you only care about the E-mail). Starting

from its middle position, which is the part most visible to your eyes. The purple border and button instead of boring white. The full storage bar making you feel like you're getting a crippled version of the service with the other options. The shiny fire button screaming at you how it's the most *"popular"* option (is it really more popular than the other plans?). Then there is the arrow pointing at the 24 month option (this ensures that, even if you find a better provider, Proton will still run away with your cash). We can add the dark patterns to the pile of reasons to avoid Proton.

But let's assume there aren't any dark patterns. The *"Mail Plus"* plan still costs more than a mail account alone should. And the free plan is useless, as it does not support mail clients. So, Proton's *"Mail Plus"* is not only outclassed by cheaper paid plans like Posteo, but also free ones like Disroot. That is even if you ignore the privacy issues. Just bury Proton already.

UPDATE October 2024: someone got me to retest broton because of some changes, and apparently you **can now sign up through the onion domain with only email verification** - and even RiseUp mail works unlike before. They still try to push you hard towards the paid account with a prompt that takes up almost the entire screen, and the only ways of paying are unsatisfactory (PayPal and credit card). Then, after you're finished, they clearly want to grab your phone number by pretending you need it for password recovery - though email alone also works. Yet it is obvious the push is for the phone, with the shiny flag and being put on top. The free account still lacks mail client support. And so, even if you can theoretically avoid the phone requirement, you still have to expose yourself to the malicious payment providers, so it doesn't end up meaning much. Anyway, I only looked at nuBroton briefly to check out the new registration process and I do not intend to do any more deep testing on it, but I still don't recommend it.

Woekli Mail

Signing up requires JavaScript and a non-empty user agent; they allege to activate your account in 48h (because of the *“huge demand”*, yeah right!) - but I've been waiting for like 6 days, and still can't login. Maybe they disliked my obviously fake name, or TOR usage...who knows. **UPDATE:** someone reported being able to sign up and login through a VPN, so this might be a TOR block during signup. Though, the actual reason a sign-up is allowed or denied is still not known for certain. He then gave me the account details and I was able to confirm a login, even through TOR - though it took a minute or more to load, so I was sure it just froze. The login screen also fails half the time with unspecific errors (*“An error occurred. Please refresh the page and try again.”*). Anyway, let's probe a little further as my handle demands. The free tier lacks mail client support, and so is doubly useless. The first paid tier costs 60 CHF (very similar value to an Euro) per year; so comes out to over 4 per month - one of the highest rates of all the providers out there. And that one doesn't even have all the features - missing custom domains and aliases. If you want that, better reach deep into that pocket for 200 CHF. Either way - if you want to get into any of the paid tiers, you need to dox yourself with *“City”*, *“Post code”*, and *“Street name and number”*. The only accepted payments are by *“PayPal or credit card”*, *“Bank transfer”*, or a *“PostFinance Card/E-Finance”* (what even is this?). Either way, no crypto, so you're getting doubly screwed. If - after all the abuses - you still want Woekli, maybe take a look at their Privacy policy (archive) (MozArchive) that doesn't actually say anything about what they store or for how long. The sign-up process also requires accepting their ToS that's in...German only. Could this big corporation existing since 2002 really not have figured out translations? I cannot imagine a reason to use (or rather - get used by) Woekli Mail; hey, it has the famous *“Swiss privacy laws”* :D. Or maybe being *“100% green”* will satisfy the environmentalists. Thanks for the assurance, but if the service itself is terrible, it doesn't mean

much.

Scryptmail (DEAD - https://blog.scryptmail.com/discontinuing-of-service/)

Free 7 day trial and then you have to pay. No mail client support. Claims to encrypt metadata and senders instead of just messages. Blog and support forum appear pretty dead; FAQ is also outdated - says Scryptmail is only a year old, but it's actually 4.

What about the privacy? Website uses Matomo analytics described in ProtonMail's section. And the mail? According to their privacy policy (archive) (MozArchive), whenever two Scryptmail accounts communicate, only *"sent times"* metadata is stored. On the other hand, if someone using another provider sends an e-mail to your Scryptmail account, the collected data extends to this:

> *sender and recipient email addresses, the IP address incoming messages originated from, message subject, body and attachments and message sent and received times.*

Other stored information includes: *"Last login time, IP address, User agent, API call."* Though they claim that they *"have no ability to match an IP to a specific user account."* Which appears to contradict the earlier claim, since they know when a certain account logged in, as well as with which IP address. It is possible they delete the information about the account which the data belongs to, but to say that they have "no ability" to connect them is a lie.

You should assume that your data will be stored pretty much forever. From the Data Retention section: *"Active accounts will have data retained indefinitely."* What about deleted accounts?

> *Your personal data shall be deleted no later than at the end of the calendar year following the year of the termination of the contract unless in an individual case specific reasons to the contract apply. [...] Moreover, the deletion of inventory and billing data may be omitted provided that legal regulations or the prosecution of claims require this action.*

In summary: paid, no mail client support, confusing and contradictory privacy policy, significant amount of data stored and never deleted. Avoid!

MsgSafe

Another one dug up by a chat member. Website doesn't work at all without JS enabled and embeds Cloudflare scripts. Then - after you turn on JS - you'll wish you hadn't when you realize the CSS has all kinds of fucked positioning (at least in Pale Moon), making the site barely usable. Usually I'd drop it right here, but I was in the mood for some suffering - and MsgSafe **provides it in droves**. As far as I can see, the service is webmail only, so we can't avoid dealing with the shitty design. It's funny how they make this seem like a virtue (MozArchive):

> *Our software works through the web and operates using open standards so you know what's happening at all times. There's no software to download, no app store to trust, there's just you and us, and you're in control.*

It's exactly the opposite, of course. Mail clients keep you in control, while a web app can be modified at any time by the provider, with the user unable to resist the change. If that wasn't enough, the privacy policy (MozArchive) is a nightmare:

> *This includes referrer pages, time stamps, page requested, user agent, language header*

and website visited.

We don't get told the duration all this stuff is kept for, either. And no information about the possible storage of mail content or metadata. The free account allegedly supports up to ten aliases, but I can't seem to find a way to actually create them. I assume the paid tiers do support the option, but I'm certainly not going to test it - the quality doesn't justify the price of $5 minimum per month (hell, I wouldn't use this crap for free). As a positive, it does apparently support Bitcoin payments, but...why? Leave it rotting along with FastMail, Criptext and the other piles of junk.

Criptext

There are so many violators popping up now that I wasn't supposed to review any more of them unless they were significant for some reason. However, this one was mentioned to me by two people and it encompasses a lot of what's wrong with E-mail services and computing in general, so I might as well get to it. Let's start with the quote from their main page:

Quite possibly the most private email service — ever

That's it - I'm sold. Of course, no violator has ever made that promise before...not at all. But let's not jump ahead of ourselves, and first check out what's actually so special about Criptext. First of all, since it's a shitty Electron "app" (literally embedding Chromium inside it), it **takes up a huge amount of resources** - much more than Claws Mail. The interface is your usual webshit and you cannot make it fit with the rest of your operating system - like an alien invader. Obviously, **forget about it supporting mail clients**; Criptext says **fuck the established standards** - we'll run our own special snowflake webshit implementation. That alone would usually be a

dealbreaker for me, but let's dig deeper. I don't seem to be able to run the "app" through either torify or proxychains, so it can be assumed to **not support anonymization**. To use Criptext, you need to sign up through the "app" which **asks you for your real name**. Now let's tackle some specific claims made on their site:

> *All your emails are locked with a unique key that‘s stored on your device alone, which means only you and your intended recipient can read the emails you send.*

So, Criptext alleges to be E2E - but actually, it only works between Criptext accounts - others will just receive your mail unencrypted as usual. And - as the "app" doesn't support PGP (unlike a regular mail client) - you're left bare unless you encrypt through the command line. This is not at all different than what Proton or Tutanota are doing.

> *Criptext doesn‘t store any emails in its servers. All your emails are stored on your device alone, which means you‘re in control of your data at all times.*

That's actually **absolutely impossible**. At some point, the E-mail has to go through Criptext servers so that it is delivered to the recipient. Why pretend otherwise?

> *With real-time tracking you can know once your email is read.*

This is advertised as a unique feature, but actually, mail clients support it with something called *“Request Return Receipt”*. No advantage for Criptext, unfortunately. Now check this from their security section (MozArchive):

> *All your emails and private keys are stored solely on your device. Once Criptext delivers*

> *an email there‘s no trace of it left in our servers whatsoever.*

This is called *“decentralized architecture”* by Criptext - which is of course a total joke since their "app" enforces usage of Criptext servers - unlike a regular mail client. Let's now check out their privacy policy (MozArchive):

> *Once messages are delivered to your device, they are deleted from our servers. The same holds true for messages which you send.*

Okay - assuming they're not bluffing (which they already did a few times) - this is a welcome change of pace compared to most violators. However, POP3 protocol in mail clients supports the deletion of E-mail upon retrieval - so again, this is not specific to Criptext.

> *We also keep email metadata (subject, date and sender email address) in order to enable certain features of the Services, such as the “unsend”, “read receipts” and “expiration” features.*

The duration is not mentioned. Red flag.

> *When a normal, unencrypted email is sent to you by a non-Criptext sender, the email gets encrypted by the server with your public key and can only be decrypted by your device. The same holds true for attachments that are sent to you from non-Criptext addresses. This means that your emails are always encrypted, even if the sender is not using Criptext.*

That just means the E-mail would be encrypted from Criptext to you - but not before it reaches

Criptext. Therefore, Criptext could still read it - again, why pretend otherwise?

> *We may automatically log information about you and your computer or mobile device when you access our Services. This includes information like hardware model, operating system information, battery level, signal strength, app version, browser information, and mobile network, connection information including mobile operator or ISP, language and time zone, and IP.*

So, Criptext stores your IP address and lots of other information. Duration is again not specified. It also shares that data with unspecified partners:

> *We may disclose your personal information to our subsidiaries and corporate affiliates for purposes consistent with this Privacy Policy.*

Okay, I think it's **lights out for Craptext** now. The only positive about them is their promise to immediately delete your E-mail upon retrieval - but seeing how many deceptive claims they've already made, it's doubtful they even do that. **All that remains from the privacy posturing on their main page is a pile of rubble**. The sane thing to do is to leave Craptext rotting right along the Protons, Fastmails and Hushmails and use some proper services.

Lavabit

I don't want to spend too much time on this, but a few people requested a review, including someone today. So let's just skip to the most important part of their privacy policy (MozArchive):

> *On a final note, the Lavabit e-mail servers do record the IP address used to send an outgoing message in the header of an outgoing e-mail. Because of this, it is possible for the recipient of a message to identify what IP was used to send a message.* ***We record this information in the message header so that law enforcement officials in possession of a message that violates the law can identify the original sender****. Lavabit does not retain this information.*

Honeypot alert! Honeypot alert! Honeypot alert! Can it get anymore obvious? **Lavabit puts your IP address in the headers for the sole purpose of allowing the government to bust you**. Consider the fact that the FBI has already busted the owner himself for running the previous iteration of Lavabit, that Edward Snowden was using. And then, he suddenly "resurrects" it, like it was nothing. The owner even admits on his media page (RT interview) that if you *"resist the government"* they can *"take everything from you"*. Yet, they allowed him to resurrect, meaning they did not *"take everything"* from him. He then says that even if he ran the service in another country, the US gov could still bust him again. Yet, they did not bust him the second time. In the freethink interview, he also says that he had to *"shut down the service"* or go to jail for disobeying direct surveillance orders from the government. And yet, **he is still operating**! Read between the lines, people. If he's still operating - and not in jail - then he **must be** doing that with the government's approval. Meaning, he must have installed surveillance to their satisfaction. Lavabit is absolutely a **prime, raw, organic honeypot**.

But it gets worse (it can't ever get better, right?). Lavabit is a **paid service** (unless you have some "promo code" - I have no idea how this option works). And to sign up, you need to give it your *"Name"*, *"Address"*, *"City"*, *"Postal Code"* and *"Card Number"*. Wow! All the stuff the gov will run away with (since we've proven above that Lavabit now works with them). If Lavabit's privacy posturing was still valid, don't you think they'd support cryptocurrency

payments, at least? But again, currently they exist only as a government honeypot. And Lavabit's privacy reputation is being used to lure the low tier privacy enthusiast right into its sweet trap. It disgusts me, but what can I do? Expose it, which I'm doing right now (but I realize it's not enough and people will still rely on the advertising). I kind of didn't bother to review this service for a long time, because I thought it's so, so obvious it's a honeypot. Even without reading policies, the out-of-nowhere resurrection - after having been shut down by the FBI before - should be enough to raise suspicion. I won't even bother to analyze how expensive Lavabit is, because who cares, really. You shouldn't be buying it regardless. With all this in mind, let's check out the media reception of Lavabit's resurrection:

- Ultra private email provider Lavabit is back online (archive) (MozArchive)
- Secure email service Lavabit relaunches, citing need for security in ‘post-Snowden world’ (archive) (MozArchive)
- Snowden's preferred email provider, Lavabit, has been resurrected (archive) (MozArchive)
- Lavabit relaunches secure email service, encrypted mail goes open-source (archive) (MozArchive)
- Go dark with the flow: Lavabit lives again (archive) (MozArchive)

And other, similarly masturbatory headlines. Wow! Is this journalism, or fanboying over your favorite sports player? None of those outlets even bother to mention the proven fact of Levison now running a honeypot, or in other words, being another Sabu (archive) (MozArchive). Is journalism just a giant masturbatory session these days? It seems so. It's so tiring; I should get a medal (or whatever) for being the only one with integrity /s.

What about the so-called "Dark Mail protocol" that Lavabit's owner invented, that allegedly fixes all the security issues of E-mail? It's a mirage! It doesn't work! He admits it, too. Look (archive) (MozArchive):

> *Currently we only support Lavabit Flow, which allows users to operate in "Trustful" mode using any POP or IMAP client. While we've developed command line tools, and libraries with DIME support, we are still working to integrate them into full fledged applications suitable for customer use.*

10 years of "Dark Mail" development, with absolutely nothing to show for it. And yet, all the media outlets salivate over this **nonexistent** thing!

Purelymail

I'm kind of tired of all the complicated political analysis I've been doing recently, so I thought I'd rest with the usual easy update, namely the taking of another shitty E-mail provider to the butchery (sorry for the spoilers). First of all, the service is paid, and the only way to pay seems to be PayPal (the *"Pay by card"* option doesn't seem to work; not that it would make it much better, since it uses Stripe). Let's remember that PayPal not only requires you to dox yourself, but they have also positioned themselves as arbiters (local) of who deserves to be able to transfer money, and who doesn't:

> *After the Charlottesville violence, PayPal pulled its services from 34 organizations the SPLC identified as hate groups (Jan 2017; Hatewatch 2017).*

Purelymail brags about being cheap ($10 per year), but so what if I can't pay with crypto? Hey,

there's a trial mode, but it requires a fucking phone number to sign up for - what a joke! And before you are even able to try it, you're hit with the message *“Calculating, please wait. This is an antispam measure that should take about 3 minutes”*. I really can't be fucked to wait so long for this shitty provider to graciously let me use it. If that wasn't enough, your password needs to get past some arbitrary rating thing before being accepted. It's funny how they claim your password would get broken in exactly this or that amount of minutes or years, as if it didn't depend on the assumptions the cracker makes. I've had it claim that my password that seemed pretty strong would be broken in minutes (don't worry, I'd never use that one for a "real" account, but I'm still certain that's a nonsensical estimate). Ugh! Just let me through, I'll take care of my password strength by myself, thank you very much!

Also, it's funny how they are still beta despite being around since early 2019. I think it's just a way to deflect fuckups. Hey, maybe I shouldn't be so harsh on this service. After all, it's run by one guy (archive) (MozArchive). And there are some positives about it. Namely, it supports mail clients (but so does Gmail). Oh, and there is no political discrimination:

> *The company will not discriminate against its users for any personal or political reason. To the extent possible, Purelymail takes no stance on any political issue. Really, we're just here to provide a service.*

Nice to know, but I think very few providers actually discriminate in this way, so not doing so is not that big of a deal. Purelymail also pretends to have good security (archive) (MozArchive)... and maybe they do, but so what if you can't get in, in the first place? And remember, you're relying on one guy to handle all that "security". Strangely, that page also says this:

> *During our beta period, we retain backups of deleted email messages for one month. This includes original undelivered messages. We do this to prevent data loss from any mistake or accident on our part.*

So, *"deleted"* means not actually *"deleted"* in the Purelymail world. Their ToS (archive) (MozArchive) also says some "interesting" things:

> *The Company may, at its sole discretion, terminate service without cause or notice. The Company reserves the right to refuse service to anyone for any reason at any time.*
>
> *Services provided by and payments made to the Company are non refundable, except at the sole discretion of the Company.*

"Any" reason? Including personal and political ones? So much for non-discrimination. After going through all the hoops this service requires from you to be able to sign up, they can just trash you and steal the money you've given them. Amazing. Then there's this:

> *The Company reserves the right to monitor, retain, or disclose any information necessary to satisfy applicable laws, regulations, or governmental request.*

Hahaha. I guess there wasn't a reason to give this service the benefit of doubt, after all.

Soverin

Another person requested a review, so here it is. Thought it's obvious it's terrible so I'll be brief here. Phone number requirement during registration makes Soverin completely **non-anonymous**

- and for me, alone disqualifies it. Privacy policy says nothing about what data they actually store and for how long - only that if you delete your account, it's all gone. Soverin **dares to ask for money** for this abuse - and through a third party payment processor (archive) (MozArchive) that collects everything possible about you and even shares it with others - *"Mollie will share your personal data with third parties if this is necessary for the performance of the contract or if it is based on legal obligations or legitimate interests"*. As for some positives - well, mail clients are apparently allowed, as well as Bitcoin. But if their payment processor stores so much stuff, does it even matter? There is disk encryption...who cares, everyone now does it. If you really want to part with your money, get Posteo that is 3 times cheaper and much better. Or just go for the good free ones like RiseUp or Disroot.

✉ Librem Mail ✉

A chat member has inquired about this one. Their modus operandi sounded nice:

> *Purism is a Social Purpose Corporation (SPC), which means we put social good above exploiting people.*

So I decided to check them out, naively believing it (I guess the Mozilla situation has taught me nothing). The amount of personal data required for getting an account is **the most I've ever seen out of any provider**:

> *Billing First name is a required field. Billing Last name is a required field. Billing Country is a required field. Billing Street address is a required field. Billing Town / City is a required field. Billing State is a required field. Billing ZIP is a required field. Billing Phone is a required field. Shipping First name is a required field. Shipping Last name is a*

required field. Shipping Country is a required field. Shipping Street address is a required field. Shipping Town / City is a required field. Shipping State is a required field. Shipping ZIP is a required field. Please enter an address to continue.

What a shitshow. And you need all this info even if trying to pay using cryptocurrency. Librem is a paid provider, and you can only pay for a bunch of services together. This is like going into a store to buy bananas, but learning you can only get them in conjunction with apples - and you hate apples. Now, if you do want their VPN, chat and social media, the price might seem justified; but this is the E-mail report and a minimum of $8 per month for an E-mail is just too much compared to even the most expensive providers. Especially since Librem doesn't seem too interested in privacy with all the personal data it's trying to grab. The signup process alone is enough to drive someone away from Librem, but fuck it, I'll dig into their privacy policy (archive) (MozArchive) anyway. Aside from the empty posturing - such as *"We do not track you."* or *"We do build products, software, and services that respect society and your privacy."* - the only mildly useful information is that they keep *"temporary"* things for 30 days. Don't expect the *"social purpose corporation"* (heh) to tell you about what exactly that consists of, though. Librem does support mail clients, which is the only real positive I can see about this service.

Swisscows Mail

A requested review. Handling cow dung again doesn't appeal to me, but I will sacrifice myself. Swisscows had already broken trust with their search engine which was famously terrible. So it's easy to expect the same with their E-mail service and that is exactly what happens. To get in, you need a Swisscows account, which requires a phone number - eliminating anyone that

really cares about anonymity. **You cannot bypass this step** in any way. But even before you get to that point, the buttons for accepting their privacy and cookie policies malfunction in funny ways, showing lack of care. Their privacy policy (archive) (MozArchive) seems to only be written in regards to their search engine - so you're in the dark as to what data their mail service collects. However - presumably - they're doing the same as with their search engine, and so:

> *We also perform statistical analysis to understand user behavior and trends, to be able to improve Swisscows and decide which features should be implemented next.*

This applies. As well as the 7-days log storage which includes *"IP and user agent"* and surely the metadata. But again, this is just guessing since they don't tell you. Their ToS (archive) (MozArchive) contradicts their privacy policy:

> *This means that your activities are in no way logged, stored or transmitted to third parties when you connect to our services. We do not collect IP addresses, browsing history, session information, bandwidth used, connection timestamps, network traffic, and other similar data.*

And as usual, you should assume that the worse option is the valid one. So 7 days logs storage. Swisscows brags every so often about their *"Swiss privacy laws"* - *"Swisscows.email was founded in Switzerland and all our servers are located in Switzerland. This means that all user data is protected by strict Swiss data protection laws."*, however those still allow (archive) (MozArchive) **direct surveillance** by the glowies. They admit this:

> *The only legitimate reason we would have to start collecting private data would be the existence of a valid judicial order or a court order that would force us to take this step.*

How it works in practice you can read about in Proton's section. Anyway, if you pay for the E-mail service, they don't give refunds:

> *If you buy our paid Swisscows services via all possible sales platforms, we will not give you a refund.*

Though stupidly (but better for the user), their free service isn't really worse than the paid one (in terms of the E-mail, at least):

	FREE	STANDARD
Users	1	1
Storage	500 MB	5 GB
Addresses	1	1
Messages per day	150	1000
Folders / Labels	Unlimited	Unlimited
IMAP settings	Yes	Yes
Support	Limited	Normal
PRICING	FREE	CHF 5.00 /mo CHF 45.00 /yr

Hey, look, **they support mail clients**! So they're not as terrible as the worst of this list. But so what, if you end up choking on the phone number requirement for registration? Anyway - if

you do want to get the paid version for some reason - you're going to have to deal with Stripe for payment processing:

> *is made according to the Swisscows user's choice by invoice, PayPal, direct debit, credit card debit (via our partner Stripe GmbH)*

And the privacy of that is absolutely terrible:

> *As allowed by law, we use and share Visitor Personal Data with others so that we may advertise and market our Services to you. Subject to applicable law (including any consent requirements), we may advertise our Services to you through interest-based advertising and emails, and seek to measure the effectiveness of our ads.*
>
> *Usage data associated with those devices and browsers and how you've engaged with our Services, including IP address, plug-ins, language used, time spent on Sites and Third-Party Sites, pages visited, links clicked, payment methods used, and the pages that led or referred you to Sites and Third-Party Sites.*
>
> *As part of these Services, you will be asked to share Personal Data with us for this purpose (e.g., your government ID, your image (selfie), and Personal Data you input or that is apparent from the physical payment method (e.g. credit card image)). To protect against fraud, we may compare this information with information about you we collect from Business Users, financial partners, business partners, identity verification services, publicly available sources, and other third party service providers and sources so that we can assess whether the person is likely to be you or a person purporting to be you*

I don't want to cite the entire policy, so go visit the link if you're still interested in learning about the abuse. Swisscows ToS also disallows this:

> *Submitting false or misleading information*

Lol. Also:

> *Transmitting content that is generally offensive, unlawful, threatening, harmful, abusive, tortuous, harassing, or may be deemed to be so in a court of law;*

Please. Let us be adults, for fuck's sake. Anyway, summarizing: Swisscows Mail **does support mail clients** in its free tier. But so what, if I can't sign-up because of the phone number requirement? So I can't even verify anything here, for real. Looking at the policies, it's clear that they've all been written in regards to the search engine, so we don't really know what happens on the E-mail side of things. This service is truly run by incompetents; they've even created a paid tier that doesn't bring any real advantage over the free one. Regardless of anything else, the phone number requirement absolutely kills this provider.

SAFe-mail (safe-mail.net)

UPDATE August 2020: The signup still requires manual approval and it's hit-and-miss whether you get in. Last time I reviewed them I didn't, even though I gave a real looking name. Now despite a troll name they accepted me for some reason - and I did it through the TOR network too. Clearly, they're not a serious service. Often, you can't even connect to the site and they send you http:// links through E-mail - which are not even redirected to HTTPS (without addons). More importantly, **full mail client support is limited to paid accounts** - free ones can

only receive. Therefore, this should be considered a paid provider, with minimum $25 per year (or about $2 / month). And if you do that, you need to provide your real name, address, and credit card data, so it becomes totally useless for privacy. Lights out for SAFe-mail then, but there's more damning information I wrote previously, so take a look at it if you want to dig deeper still:

Israel-based service established in 1999. Before I delve deep into the meat of the issues, let's look at the first impression. Namely, **the site structure and grammar is something a chimpanzee would make** - this makes getting any information from the site a puzzle in itself. Most of the stuff in there is ancient, and some sections contradict each other. They've had **20 fucking years** to make a proper website but instead we get this abomination...but let's try to make sense of it anyway:

SAFe-mail pretends to be privacy-based but has no real privacy policy. The only thing is a snippet **from 2008** saying:

> *Safe-mail.net is not using cookies and not collecting any data about users. Safe-mail.net does not transfer, sell, trade or oterwise exchange any data it might have about its users with any other company.*

So it allegedly does not collect ANY data about its users. Why, then, do they bother to qualify it with a statement that they also don't sell the data? Wait, there's also this: (from the user agreement) (archive) (MozArchive)

> *SAFe-mail Ltd. will not disclose information about you or your use of the SAFe-mail system, unless...*

Okay, so you DO have data about your users after all...

> *You agree that SAFe-mail may access your account, including its contents, for these reasons or for service or technical reasons.*

So now you admit that you can access even the contents of my account? Isn't this an admission that you read our mail?

> *Please note that your Internet Protocol address is transmitted with each message sent from your account.*

No shit. But what we're interested in is whether that IP, or any other data, **is stored by SAFe-mail, and for how long** - and this information is not provided. Does this not sound suspicious? SAFe-mail spends a lot of time posturing on how privacy-based it is, yet seems strangely secretive about the kinds of data it collects; in fact, you have to read between the lines to realize that it stores anything at all. A clear indication of a **honeypot** to me.

OpenMailBox (DEAD)

Has **no privacy policy at all** - a huge red flag; in fact, all they really say about privacy is that *"all user data is stored in privacy respectful countries"* - without, of course, specifying those uber-private countries. ReCaptcha is required to sign up, which shows you just how much privacy matters to them (if they submit to the Big G's botnet, you can safely assume they store fucking everything). Openmailbox severely lacks ethics, deleting features without notice (MozArchive):

Free users of Openmailbox could use IMAP/POP to connect to their mailboxes previously. The new owner of the service, French company SASU Initix, disabled the option without prior notice for all free account owners.

This blocked the use in all email clients for free users, and left them with no choice but to use the web interface instead to do their mailing.

Related to that is the removal of the mail aliases feature. The available aliases were removed completely and stopped redirecting any messages.

Imagine you've used an alias to talk to your family and it suddenly stops working - so you don't get their messages anymore, unaware of the reason it happens (hey, maybe they hate you now...). They also claim you can make an account in a minute - which is simply mockery due to ReCaptcha. Their Terms of Service (archive) (MozArchive) follow the same principles (or lack of):

OpenMailBox reserves the right to amend this text, without prior notice, and you are therefore responsible for making yourself aware of the latest version of this text. In the event of a breach of these conditions, your user account may be locked or deleted, with no option for redress or compensation.

So if they suddenly decided VPN / TOR users are dangerous terrorists, they will kick you out just like that; say goodbye to your contacts, messages, everything (since mail clients don't work, you can't easily download them). Free accounts inactive for 180 days will also be deleted.

There is a rumor going around reddit that either OpenMailBox or Autistici gave access

(archive) (MozArchive) to someone's account to the Singapore Tax Authorities. However, this is almost impossible for Autistici since it would go against everything they've always stood for (archive) (MozArchive):

> *After 2005 we have been constantly pestered by prosecutors and security forces (and even by the Vatican! [4]) asking us to hand over users' data and identities and we are proud to say we were always able to answer: we are sorry, but we do not have them. Recently (2010) some very smart policeman managed to convince a judge to order the full seizing of three servers in three different countries to find out if we REALLY did not have any data about a user's activity on our servers [5]. After spending a lot of public money (for a couple of graffiti on a wall), the judge ended up with a lot of encrypted files with no useful information inside, and maybe he'll think twice about giving out other investigations to the cunning policeman.*

On the other hand, it would be quite consistent with OpenMailBox's proven lack of ethics. But, in the end, it is just an unconfirmed rumor - so take it with a grain of salt (however, the person did post it more than once).

In short - no privacy policy, no mail client support (for free accounts), no respect for the user. Just a cash in for their premium service which still doesn't guarantee you any privacy (in fact it's a possible honeypot for governments). No reason to use this at all when you've got other free services available with more features, better privacy, and actual ethics.

 Runbox 

Their website is so full of privacy posturing it's a wonder how they managed to fit anything

else. I won't bother quoting it all here; let's move right on to seeing whether the posturing is actually worth anything (spoiler: it isn't). From their privacy policy (archive) (MozArchive):

> *You consent to providing us with the following personal data when you register an account: First name, last name, company name (where applicable), mobile phone number (where applicable), country, and alternative email address. [...] To revoke this consent you must terminate the Service*

Sorry Runbox, but requiring my real name just ain't privacy-respecting. The first impression already isn't very good...and it's just the beginning. **UPDATE February 2023**: didn't care about this provider for a long time, but someone notified me that this data can be faked and / or removed after registration. I never actually tested it as I lacked an account, and Runbox is paid. I also have no means of confirming if they do care that you fake it. Still a bad omen that they ask for this data in the first place.

> *Your Account Information is stored on servers located in Norway for as long as your account is active...*

Great, so I have to kill the account for you guys to stop storing my information. And then it's fucking gone, right?

> *...and: up to 1 month after closure of trial accounts; or up to 5 years after closure of subscribed accounts, as financial records must be kept for 5 years according to the Norwegian Bookkeeping Legislation.*

No, of course it isn't fucking gone - that would be too private for the "privacy-loving" Runbox.

So it's five years after the deletion of your account until your real name is gone from their database...or is it?

> *Backup of Account Information is stored on secure servers separate from the Runbox system for up to 6 months, even after the information has been deleted from the main storage.*

Nope, the privacy-loving Runbox is truly smashing all the previous privacy records set by privacy giants such as Google or Yahoo; it's **five and a half years until your data is gone from their servers**! Oh Runbox, what are some other ways in which you protect my privacy?

> *Email service content (data associated with Webmail, Contacts, and Files in the Service) is stored in main storage on servers located in Norway for as long as your account is active and: up to 3 months after closure of trial accounts; or up to 6 months after closure of subscribed accounts.*

So all your mail and metadata (sender, recipient, subject, date/time) is stored as long as your account exists. There's also the backup which is stored for longer. Should we prolong this torture? Okay, let's do the finishing move and get this over with: The Runbox "service" is **fucking paid**! Can we say **final nail in the coffin?** Seriously, they're like a Gmail you have to pay for...but wait, there is more: (I swear it's the last quote!)

> *If you correspond with us via e-mail, the postal service, or other forms of communication, we will retain such correspondence and the information contained therein.*

To say something positive, I will mention that they accept Bitcoins...and you can use them through the mail client. There is also a 30 day "free" trial. Oh, and they are powered by renewable energy sources (but so is the actually private Posteo, reviewed later), which is the only really commendable thing about this "service". But since the data collection and storage policy is so terrible, you should stay away.

Mailfence

It's August 2020, time for an update. First, let me say that **I could not sign up** despite enabling cookies, JabbaShit, XHR and filling out all the fields correctly several times. Was the issue Pale Moon or maybe the VPN? Who cares - if I can't register, the service is useless. Free tier does not support mail clients so for MailFence to be even slightly worth bothering with, you need to pay (2.50 € per month, Bitcoin accepted). Of course the front page contains privacy posturing:

> *We believe that online privacy is a fundamental human right which can no longer be taken for granted so we decided that it was time to offer a service which is fully dedicated to email privacy.*

I've heard that before. Let's see how this claim stacks up with your privacy policy (archive) (MozArchive):

> *We implement a local instance of Matomo [...]*

This crap again. Read ProtonMail's section to see just how vile it is.

> *We collect IP addresses, message-ID's, sender and recipient addresses, subjects, browser*

versions, countries and timestamps.

Already a red flag here. No mention of how long this data stays around, but we do have an idea of how long they store your E-mail:

We retain backups of deleted messages and documents for 45 days.

Very private you are. And then comes this excuse:

This is for the purpose of restoring data in case of accidental deletion by users. After 45 days, data will be permanently deleted from all our systems.

Yeah sure - it's always for the user's good. In the end, **your deleted mail will stay on the servers for 45 days**, regardless of justification. And if that wasn't enough...

Should you close your account, all data will be permanently deleted 30 days after the legal expiration date (i.e. the Belgian law imposes 365 days after account closing).

So you have to **wait for over a year for your "deleted" account to be actually deleted**. Belgian privacy laws in action! Summarizing: the service stores a lot of data and is strangely secretive about the duration - but we can guess it's somewhere between 45 and 395 days. Mail client support requires paying, and if you're going to do that, there are much better options. So, forget about MailFence.

Safe-Mail (safe-mail.nl) (SIGN UP DISABLED)

Let's move straight to the meat of the issue:

> *The Safe-Mail Team are a bunch of nerds with a clear vision about privacy. And we want to give others the opportunity to protect their privacy. With a Safe-Mail community we want to let the world know that privacy is a legal right and we are ready to fight for it.*

Great, and yet...

> *The provider does not check on messages or any other content stored on Safe-Mail.nl unless bound by law to do so (this means only when we get a court order!!).*

So you **can** check on messages? Anyway, they will not fight court orders. So much for the *"privacy is a legal right"* posturing.

> *We do not hold any user information accept for the information you give us at the registration.*

Unfortunately, that information includes my real name and city (I guess I can give a fake one, but still...).

Safe-Mail.nl does not have a true privacy policy, so all we have to go by is the above snippets plus a section from their FAQ - *"What do you log?"* - which says:

> *The whole Safe-Mail system is using different log files which we need to access when there are problems with the system. It's called maintenance and important for the health of our Safe-Mail system. We totally understand that it feels uncomfortable by the idea*

that you aren't really anonymous then, but we also cannot say that we log nothing. But we are convinced that log files older then 7 days does not have any value to us. Especially when it contains maintenance value. So we decided that all logs with "specific" information are being deleted from the server after 7 days. Log files only takes up space and we want to save that for more important matters. That does not mean you can abuse the system. There are rules and our guess is that all of you know what those rules are. We fight for privacy here, but we condemn illegal activities. Please, think wise and twice when you use the Safe-Mail system.

Not many specifics - remember, **secretiveness is a red flag** - but "specific" data (whatever that means) allegedly stays around for only 7 days.

Free account does not support mail clients. They do accept bitcoins so theoretically, you can have an anonymous account with mail client support. Even in the free account, you can upload an S/MIME certificate to have end-to-end encryption, however, unlike PGP, **this relies on trusting a certificate authority** - similar to SSL.

Maybe I'm a little too harsh on this one - but if FREE services with mail client support are available - that also don't ask for your real name - and will ACTUALLY stick their heads out for your privacy - then those should be used.

Neomailbox

Paid only - 50$ per year; bitcoins accepted. Mail client support. TOS forbids you from badmouthing the service (lol) - *“not publish or post false, malicious, defamatory or libelous comments about Neomailbox or Neomailbox Customer Support in any form online of offline”*.

What about the privacy? Not much is mentioned except:

> *We keep logs of SMTP traffic for 6 months for performance analysis and abuse prevention. Anonymous surfing logs are wiped every 10 minutes.*

This used to be 2 months, so they multiplied the duration by 3. And the specifics of "SMTP traffic" are not mentioned so you should assume it's absolutely everything. And in another part of the website:

> *We keep no logs or customer data other than what is absolutely necessary for performance tuning and security monitoring of our servers. Your IP address is not saved in our logs. All logs are deleted every 7 days.*

UPDATE: **the IP part is not in the FAQ (archive) (MozArchive) anymore**, roundabout confirming they do store your IP. But wait, that contradicts the earlier quote. So they didn't explain themselves clearly - that's a red flag; as if they didn't want you to know what exactly they store. You should assume the worst - namely that **all your mail content and metadata is saved** for 180 days. There is also this:

> *The following statement is true on January 1st, 2020: Neomailbox has never released any customer data to any government agency or other entity.*

That's nice. However, the fact is - not only do you have to pay for getting your data stored for half a year, but cannot even say a bad word about them. For something positive, Neomailbox has disk encryption and unlimited aliases. Still, they are paid, keep your unspecified data for 6 months, and have weird stuff in their ToS. My friend has also proven that one of their mail

servers **fails the TLS test** - which means your mail is sent around unencrypted. You could do much worse than Neomailbox - but also much, much better.

✉ Mailbox.org ✉

UPDATE March 2024: lots of stuff about this provider apparently changed, so I might as well re-review it though I don't really want to.

First of all, this is a **paid provider** (there is a free trial but it's worthless as you can only message other Mailbox users) - and crypto is not an option. Though you can apparently send cash by mail anonymously, like with Posteo. Still, no crypto is a significant thorn on Mailbox's side. Let's dig further though, for maybe it justifies itself later:

On the first registration screen, you need to enable cookies to proceed, even though uMatrix shows no cookies being set. On the second registration screen, you input username and password (no JS needed here). The third registration screen has this "friendly captcha" thing for which you need to enable third-party JS. Then, the captcha solves itself in two minutes or so. That's a lot better than hCaptcha or reCaptcha would be, of course. But still, it's a third party request. Mailbox asks for name and surname, but it can be faked and they don't care.

Just in case you were getting comfortable, Mailbox works closely with the feds (archive) (MozArchive):

> *When you register on our internet pages, the IP address assigned by your internet service provider (ISP) as well as the date and time of the registration are stored. This data is stored because this is the only way to prevent misuse of our services and, if necessary, to*

> *enable us to investigate criminal offences committed. [...] This data will fundamentally not be shared with third parties unless required by law or for the purpose of criminal prosecution.*

According to their transparency report (archive) (MozArchive), 133 government requests were fulfilled by Mailbox in 2023 (130 of which from the German government). It seems that they just give the feds full access: *"or present a judicial warrant that asks for the release of mailbox contents and data logs, or order the surveillance of the user's telecommunications data"* including future access. So, I don't recommend Mailbox if you're going to fight the government, especially the German government. This, for me, **totally disqualifies this provider**. Though it might seem like a joke to speak about those after all this, there are actually some positives in terms of Mailbox's privacy. There isn't third party sharing for example:

> *The data stored by you is used exclusively for the aforesaid purposes. Your data will not be used for other purposes, evaluated or shared under any circumstances. A sharing of the data with third parties is excluded.*

And, there are quite detailed explanations of which data is stored and for how long, but we will not analyze that here. You can also request to be shown what data Mailbox has stored on you, and it will display (though, obviously, it's not all of it). It's nice in that I haven't seen this approach used anywhere else.

Mailbox has aliases. The cheapest plan (€1 per month) only allows three, which clearly isn't enough if you want to use this as your regular provider. So you effectively need to grab two additional euros from your pocket for this functionality. The aliases appear to work properly, as in, the actual address is hidden from the recipient.

As I've done for many other providers, let's see if it's possible to fish out some interesting things from their ToS (archive) (MozArchive):

> *the storage or the dispatch of pornographic material as defined in Sections 184-184c of the German Criminal Code (StGB) or of media listed in Section 24 Paragraph 1 of the Youth Protection Act (JuSchG) as being harmful to minors.*
>
> *the storage or the dispatch of image, video, audio, text or other files in contravention of copyrights, trademark rights, name rights, competition rights or personal rights or of files which contain prohibited propaganda material or designators of unconstitutional organisations (Sections 86 and 86a of the German Criminal Code [StGB]) and*

Wow, that's quite the short leash Mailbox keeps their users on. Can't be bothered to examine those laws in depth but looks like piracy is banned as well as any opinion that bothers the government (I suspect that's what's hiding behind *"prohibited propaganda material"*). Another big strike against this provider, for me. Anyway, to be thorough, Mailbox has 2FA and a bunch of functionality other than mailing that I don't care about. Mail clients are - maybe surprisingly - supported! Still too many flaws for me to bother with this provider. Namely no crypto support, a useless free trial, significant ToS restrictions and hugging the government a little too closely. Also, how the fuck was I supposed to guess that the settings are hidden behind the *"Customize this page"* option?! Totally unintuitive.

✉ Secmail.pro ✉

UPDATE July 2021: Dead. Rumors of the admin being arrested (MozArchive), but no proof.

Onion-only provider accesible through http://secmailw453j7piv.onion. No mail client support. Signing up is hassle-free with simple captcha and no personal information required. Keep in mind that - even though connecting through onion means that your IP address likely won't be revealed - **secmail could still read the mail contents** unless they are PGP encrypted. Since the TOR network is a very tasty target for various spies, it makes secmail's trustworthiness all the more important - and unfortunately, they fail the test. The service contains **no privacy policy** - though it has some vague claims of really caring about your security, there is **zero information on what they store and for how long**. Their clearnet domain contains just a link to the onion - however, it **has no SSL** so an attacker could rewrite the link to their phishing site and steal credentials. In fact, this is how SIGAINT, another onion e-mail provider, got hacked sometime ago (archive) (MozArchive):

> *We are confident that they didn't get in," states the alert. "It looks like they resorted to rewriting the .onion URL located on sigaint.org to one of theirs so they could MITM [man-in-the-middle] logins and spy in real-time."*

Another investigator wrote them an e-mail (MozArchive) a few days ago where they said that they have no time to implement SSL (they are relying on the TOR network's automatic bad relay detection, which is not perfect (MozArchive) - *"In 32 days I've found 15 instances where a node is sniffing and using my credentials"*). They've had **two fucking years** to support SSL but don't - and since they know about SIGAINT's hack, making themselves intentionally vulnerable to the same means they are either be heavily incompetent or **a honeypot**. Secmail has also refused to comment on not having a v3 (more secure) onion domain; do they also not have time for that? All it takes is one additional line in the config file (archive) (MozArchive): *"Just use your regular onion service torrc and add HiddenServiceVersion 3 in your onion service torrc block."*.

When secmail got started, they advertised themselves on reddit (archive) (MozArchive), where they took a lot of criticism. For example, their first server configuration **used to reveal the OS and PHP versions**, which makes it so much easier for hackers to get in - and at that point, they were already *"operating for more than six months"* - can you say incompetent? So, despite allegiances of security and the allure of the darknet, I'd stay away from this one. It has nothing at all over RiseUp which also supports onion domains (v3 as well!). Read a deeper investigation of secmail here if you're interested.

CTemplar (DEAD)

UPDATE April 2022: Dead. No reason given as far as I can see. **UPDATE May 2022**: okay, we now know they have been threatened by the glowies (MozArchive) - *"When we created this service, we made a promise to ourselves that we would shut down the email service if we couldn't guarantee our security claims to our users. That day has come, and we would rather shut this service down than make security changes that would have been harmful to you."* RIP.

UPDATE February 2022: CBF writing a new review but now the free account requires an invite code. The paid ones cost too much for a service that **does not even support mail clients**.

I used to have a review of this one, and it was not so good. However, after reading my review, CTemplar wrote me an E-mail to say they've changed most of the offending issues (kudos!). Since I didn't want to spread wrong information, I took the old review down, and just now finally got around to a rewrite. So, is CTemplar actually worth using now?

I would still say - **not really**. First of all, it **lacks mail client support** which for me is the most important issue. I don't care about webmail when it will never have the amount of features my

mail client does and requires enabling potentially malicious JavaScript in the browser. But wait, CTemplar claims that they cannot do that because of checksums:

> *Currently all end to end encrypted email services can hack their own users and decrypt all of their data except us. We are able to provide this level of protection using an implementation of checksums that have not been used before.*

There are two problems with this claim. First of all, comparing checksums doesn't require any special implementation - you can do it with any service that shares their code externally (for example, on Github). Then, you just compare that code to the one from your browser's *"View source"* option. However, all the E-mail providers I've seen **don't actually share the code that runs on the site** - only files to build / generate it. Thankfully, one of our chat's regulars undertook the job of building CTemplar and after several tries, still couldn't. Even if you did manage to do so, you'll have to compare the checksums every single time you use the site and for every single script it loads. Clearly, this is impossible in practice, and therefore useless. If they really cared about this, they'd just put the real code on GitHub so you could compare directly.

Of course, even if you managed to accomplish the above Herculean feat, this **would do nothing to guarantee that the code is not malicious**. You'd still have to go and inspect it to see what it does, and it's made all that much harder if it is obfuscated - which CTemplar's **happens to be**. Even though they might not be able to target you specifically without being exposed through the checksums (that is, if you happened to compare them at that moment) - they can just **attack everyone**, and then even remove the violating code the next day before anyone detects it. See? Checksums do nothing to protect against malicious code. Okay, enough about checksums, let's check out their privacy policy (archive):

> *When you visit our website, your browser sends us your user-agent and IP address. When you leave our site no records are kept of your IP address with association to your account. We store your IP in an anonymous way for 7 days.*

The "anonymized data" rears its ugly head again. What exactly is stored is anyone's guess.

> *If you choose to delete your account, everything is deleted and no records or backups kept.*

Now that's a great policy which unfortunately most providers don't follow. By the way, this is apparently thanks to the *"Icelandic privacy laws"* - which are **actually a thing** unlike, say, Swiss privacy laws (a meme at this point) which enforce 6 months of data storage.

> *We will not disclose anything to third parties, except your payment information if you choose to buy a paid account.*

Again, this is the only way to be private. CTemplar, by the way, also allows bitcoin payments so even if you DO want a paid account, you can avoid your data being stored anywhere but CTemplar.

Okay, I've skipped some sections because I want to cover the most important part in depth. Check out this quote:

> *We use a CDN service because its use is required to provide a better experience serving our static website content quickly around the world. Our CDN service also provides necessary protection against DDOS attacks. CDN's can theoretically serve malicious*

> *code to our users. Our SRI & Checksum implementation offers protection from malicious code served by CDN's.*

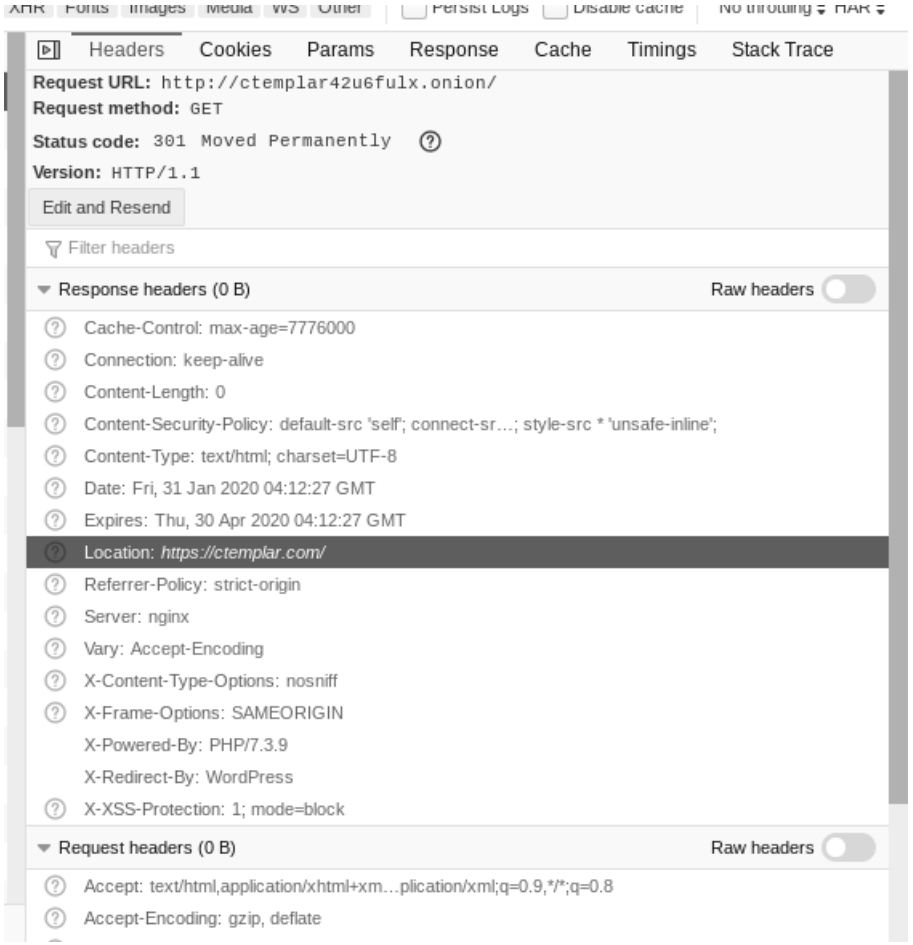
The checksums thing I've analyzed above, so let me tell you briefly what is SRI. Whenever a site includes a resource from a third party (let's say, a JavaScript library or a style) - that third party could in theory **modify the file being sent** at any time. To protect itself (and the viewers), the site could attach an *"integrity"* parameter to the resource with a hash which your browser would then compare to the received file to ensure it's what the site intended to send. If the hash doesn't match, it means that the either the site serving the resource, or some other third party, tampered with the file. However, this works **only for the resources for which the site added the integrity tag** - the meddling third party could still modify anything else. The bigger problem, though, is what kind of CDN did CTemplar have in mind (archive):

> *For example, if CTemplar receives a DDOS attack that we are not able to handle, we will switch to using Cloudflare.*

So they will put their site behind the evil Cloudflare in case of a DDOS. What does that mean for their claims about SRI? Briefly, what Cloudflare does is **proxy the whole page** (instead of a specific file or several) - so that it can **modify it before serving it to you**, including **removing the integrity checks** if it wanted to. See, SRI can only protect against the third party modifying a file **if it has no access to the page that sets the integrity checks** - but Cloudflare does. That CTemplar pretends otherwise means they are either lying to you or didn't do their research - which is bad news for their trustworthiness.

With that out of the way, let's get to the positives about CTemplar. Registration requires no personal data or ReCaptcha. Front page claims that they *"never track your IP address, keep logs*

on your usage or record any identifying information at any time"; which is great but again - since they've specified *"identifying information"*, there must be collection of some allegedly non-identifying data - and we're in the dark as to what it is. CTemplar does provide an onion domain but it **redirects to their clearnet one**:



Wow! And here I was thinking I'll be a good guy and list some positives, but it seems CTemplar **does not deserve it**. I could dig deeper, but it seems fruitless at this point. CTemplar does seem to care about you at least a little bit - since they did send me an E-mail some months ago and changed some of the offending issues. But they still don't support mail clients (the most

important feature for a provider) and have other glaring flaws such as the totally insecure and disrespectful downgrading of the onion domain to the clearnet. They also made wrong claims about both checksums and subresource integrity - call it fraud or incompetence, I don't care. Even if they changed stuff again, the **reputation has been irreversibly damaged**. As much as it pains me to say it - because there are truly lots of way worse providers out there - **avoid CTemplar**.

KolabNow

Paid, requires real name and an existing E-mail address to activate. Accepts bitcoin. Full of privacy posturing, complete with the claim of being protected by strong Swiss privacy laws. Such as this one (archive) (MozArchive), for which they've gotten a government data request that they complied with:

> *Damage to data 1. Any person who without authority alters, deletes or renders unusable data that is stored or transmitted electronically or in some other similar way is liable on complaint to a custodial sentence not exceeding three years or to a monetary penalty. If the offender has caused major damage, a custodial sentence of from one to five years may be imposed. The offence is prosecuted ex officio. 2. Any person who manufactures, imports, markets, advertises, offers or otherwise makes accessible programs that he knows or must assume will be used for the purposes described in paragraph 1 above, or provides instructions on the manufacture of such programs is liable to a custodial sentence not exceeding three years or to a monetary penalty. If the offender acts for commercial gain, a custodial sentence of from one to five years may be imposed.*

I don't understand exactly what the above means - sounds like hacking but could be interpreted in many ways (even deleting your own mail could fit *“deletes or renders unusable”*). I explore the "laws" issue in-depth at the end of this article, so let's move on to KolabNow's privacy policy (archive) (MozArchive). It says literally nothing about what data do they actually store aside from *“We [...] guarantee you that there is no third party access to your data.”* No information about the length of data collection or the possibility to delete your account and what does it actually do. Maybe we can find something in their TOS (archive) (MozArchive) then:

> *We will only keep the minimum of logs and debug information necessary to ensure that we can improve the service and resolve issues that may have occurred.*

Minimum of logs - yeah, that tells us a lot. Umm...maybe their Legal Framework (archive) (MozArchive) page has something more concrete?

> *These are requests for retained data. Switzerland has a legal requirement for six months data retention by the provider. Data that is retained is communication metadata, so information about who communicated with whom from where and when but not the actual content of the communication.*

Swiss privacy laws in action - but at least we now know something about KolabNow's data collection. By the way, their transparency report has been last updated in 2017, so they might have gotten more requests since then. In fact, the whole site appears to be dead (even their Twitter). In summary, I don't see a reason to use this one - paid, asks for real name, stores 6 months of metadata and doesn't reveal anything useful in their privacy policy. Why can the free RiseUp manage to store metadata for only one day - despite being hosted in the allegedly un-

private United States - while the service with super strong Swiss privacy laws cannot? Supporting mail clients is KolabNow's only positive it seems. That, and I guess accepting bitcoins - but since you can find better providers that are free, why bother?

Teknik

UPDATE October 2024: dead.

Requires an invite code to register. Supports mail clients. Has a nice feature of (I assume) displaying your public PGP key to others if you provide it. The privacy policy does not say much, however:

> *We use Piwik to track user interaction with the site. We keep it hosted on the server locally, so no analytic data is leaving the server.*

Piwik has changed its name to Matomo recently, so just read ProtonMail's section to know more about it.

> *Dates - When you perform an action (ie: register an account), the date of the action will be recorded.*

I assume this goes for all actions? Then it's absolutely terrible. What comes next?

> *Emails - Any email you send or receive with your Teknik.io email address is stored locally onto the server. These emails are not read.*

Thanks for not reading my mail...and that's it for Teknik's privacy policy! No mention of whether the deleted e-mail is actually deleted, if there are any backups, what kind of data is shared and under what conditions. Nothing whatsoever! Pretty suspicious if you ask me. IMO, it's not even worth bothering to get an invite code for this, when better alternatives exist that don't require it. NOTE: The webmail can conflict with the LinkBot extension if you use it, so disable it for this website.

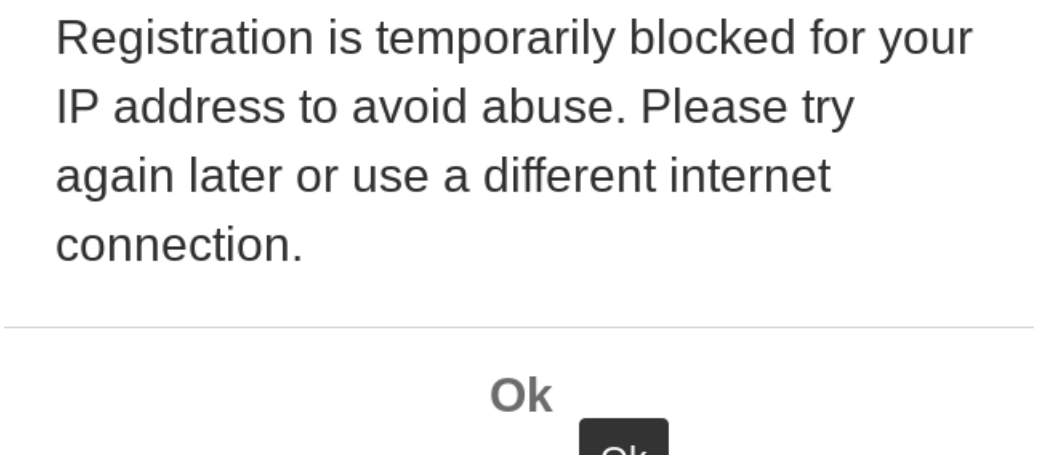
Tutanota

UPDATE February 2020: Everything is as it was but added information about Tutanota blocking anonymizers. With that, lack of PGP and mail client support, it is **absolutely useless** regardless of its privacy.

This was my first provider after I got concerned about privacy and dumped Gmail and friends. That was before I "dug deep" - needless to say, I don't recommend it anymore. **It does not support mail clients**; I used to think that's something dinosaurs use, but now I can't live without it. Encryption works only if you pre-shared a password with your recipients (unless they also use Tutanota, then it's automatic) - and that, of course, comes with its own issues (how to share the password securely?) which PGP has already solved. And since Tutanota is only accessible through webmail or their shitty desktop client (which is the same as the webmail it seems), they could easily modify the code to send themselves your password and be able to decrypt your shit. Tutanota does not support the usage of other encryption, like PGP (and in fact shits on it on its website (archive) (MozArchive), even though it's the only real E-mail encryption you can have). Unlike with ProtonMail, **there has been no third-party audit of Tutanota's encryption**. There's also this worrying policy in regards to logging:

> *In order to maintain email server operations, for error diagnosis and for prevention of abuse,* ***mail server logs are stored max. 7 days****. These logs contain sender and recipient email addresses and time of connection but no customer IP addresses.*

No IP addresses? Great! Except if you use a VPN or TOR - *"Storage only takes place for IP addresses made anonymous which are therefore not personal data any more."* It's a genius excuse, isn't it? You've hidden your IP so it isn't personal...except if TOR or the VPN ever got compromised. Also, later you will learn how just the metadata (which Tutanota does store) can reveal much more about you than you'd ever guess. This is all assuming you **can** actually use a VPN or TOR, but **Tutanota provides no such option**:



The above message appears both with the Snopyta VPN as well as TOR Browser - therefore, there is no anonymity with the uber-private Tutanota. Signing up is free, but you are limited to only one account if you don't pay. If you do, then prepare for this:

> *For the execution of credit card payments your credit card data will be shared with our payment service provider Braintree. This includes the transfer of personal data into a*

third country (USA)

Later they say that they have an "agreement" with this company that they will only use your data for the processing of the payment - but the value of these "agreements" is doubtful, in my opinion. Your payment data is also stored for whoever knows how long:

> *Order-related data and the addresses associated with the order are stored in respect to tax, contract and commercial law retention periods and erased at the end of those periods.*

Summary: **blocks anonymizers**, no mail client or PGP support, stores your anonymized IP and metadata, indefinite (?) storage of payment data. Yet another privacy giant bites the dust.

* Autistici *

A service for *"activists"* that starts off with some nice quotes:

> *We believe that this world is far from being the best world possible. We respond to this by providing activists, groups and collectives with platforms for a freer communication and digital tools for privacy self-defence.*
>
> *Our principles are fairly straightforward: the world should not be run on money, but it should be rooted in solidarity, community, mutual help, equal rights and freedoms, and social justice.*
>
> *We believe that communication must be free - and for free - and, therefore, universally accessible.*

But then goes off the deep end with an extremely restrictive policy (archive) (MozArchive) required to use it - banning, in particular:

> *discrimination based on gender, race, religion or sexual orientation*

Which is all well and good except it's historically been used to, for example, ban cosplay (archive) (MozArchive), memes (archive) (MozArchive), or hand gestures (archive) (MozArchive). Let's go further:

> *Using the Services in order to promote institutional political parties or any other organization that already has the financial resources to widely spread its own content and ideas*

Speaking in favor of a politician is a sin according to Autistici.

> *Using the Services for any military purpose, including information or training material about firearms and related combat techniques, cyberwarfare, weapons development and manufacture.*

Forget about self-defense related content, too. And the funniest:

> *Using the Services for cryptocurrency related activities;*

What's wrong with cryptocurrency? You'd think it would be considered a (relatively) anonymous and uncontrolled alternative to bank accounts. Anyway, we don't know what exactly they mean by *“promoting political parties”*, for example - so the severity of what's

accepted by the ToS is unknown. Either way, if they detect you violating the policies, you're out:

> *if we see that you're violating our principles publicly while using our services, we won't hesitate to delete your account without previous notice.*

So, you better agree with them or get good at lying / hiding. You can read more about Autistici's beliefs in A short short tale about why we are who we are and why we do what we do (archive) (MozArchive). Now let's move on to the newly written privacy policy (archive) (MozArchive) (which Autistici has **lacked for the last two decades**). Starting with the bad:

> *In order to detect abuse of our email services, we keep track of email metadata (message sender and recipient only) for every message that goes through our systems. These logs are retained for 15 days.*

Metadata is extremely revealing - enough to kill people (archive) (MozArchive) because of it. And why is it necesary to store it for 15 days when other privacy services like Disroot manage with just 24 hours? Now, since this is the E-mail report, I will only briefly cover their policy for other services they provide:

> *Whenever you interact with our platform or Services, whether you have an account or not, the automatic exchange of information between your client and our servers will provide us with some non-personal data, including, without limitation, data relating to the browser you are using (browser type, whether it is a mobile/desktop device, OS version, preferred language), the date and time of your visit and the referring website, but not your IP address.*

I've written before about the perils of *“anonymized data”*, so I will only respond briefly. All the data Autistici collects is certainly vulnerable to browser fingerprinting, and we don't know what their alleged anonymization consists of. *“Referring websites”* could also be used to create a profile of someone's interests to possibly connect it to their real life identity. How about the good stuff?

Autistici controls their servers and uses disk encryption. When you delete your account, it's fully gone in 3 days. There's no third party data sharing. Personal information is not required to sign up, but you need to fill a request - which they will check if it agrees with their beliefs, such as:

> *We support individuals, collectives, communities, groups and so on whose political and social activities fit within this worldview and who share with us some fundamental principles: anti-fascism, anti-racism, anti-sexism, anti-militarism. And on top of that, one has to share our basic attitude towards money and the capitalistic world: a deep feeling of uneasyness and unrest.*

They're really serious about this, so much that **I was asked twice** that I really am on board with their ideology before they let me through. As said before, Autistici will **kill your account** if they find you doing something contrary. In other parts of their site (archive) (MozArchive), they claim that they keep **no logs at all** - but I guess that is now superceded by the the recent privacy policy.

Autistici has an onion domain that doesn't seem to work very well. When I wrote them an E-mail notifying them of their onion failing, they ignored it. Recently, the Autistici E-mail service also been **down for a few months in a row**. Sure, I get it - you're funded entirely by donations,

whatever. Still, surely you could have gotten someone to fix stuff up in a much shorter timespan? All in all, for a primary account, **I don't recommend Autistici anymore** - though of course it's still superior to the big privacy violators. But with services like this, **it's always a danger that someone will rat you out** for violating their ideology, or they will find that out themselves somehow. So, unless you're an all-out SJW activist, you'll have to worry about self-censoring. Though, with how incompetent Autistici seems to be (being down for half a year, and having **wrong information in their privacy policy** before I reported it to them - despite allegedly being written with the help of several lawyers), it might not be a real problem. Remember, also, that even non-ideologically focused services have heavily restrictive ToSes - just maybe in some others ways. So, it's a case of pick your poison most of the time. Autistici has been around since 2001 and have a mission, so they will surely stick around, at least.

sp StartMail sp

Paid ($5 / mo, 5 times more than the better Posteo and Elude) with a free 30 day trial. Funnily, the webmail tells you you can't send mail - but it does work with the client. JavaScript is required for logging in. TOR is allowed, but provides no onion domain. Paid version has disposable e-mail addresses (a'la airmail) and OpenPGP encryption. But as usual, the most important issue is their data collection policy. Do they actually follow their *“Privacy. It’s not just our policy. It’s our mission.”* slogan? Let's find out. First, their website:

The data that's collected and processed by their website include: your IP address, browser and operating system type and version, browser language settings, country, date and time, origin of your visit, as well as clicked links and visited (parts of) pages of their website. Hmm, the latter sounds suspicious. Wonder how do they justify it? *“ to help us get an idea of which of our*

pages appear to be effective to inform our visitors”. How about the origin of your visit? *“to assess the success of our search engine optimization and information outreach efforts.”* And the country? *“to know in which countries and at what moments our marketing efforts appear to be effective.”* Sounds like **good old tracking** to me. They claim this data is then "deleted or anonymized", but whatever. I don't know about you, but I don't want to be apart of their "marketing" and "information outreach" experiments - anonymized or not. How about the mail service?

The big problem: StartMail's privacy policy (archive) (MozArchive) is extremely long, and yet manages **to not say what it actually stores** (or the duration). All that we're told is what happens when you delete your data:

> *When you delete an email, it is immediately deleted from our production servers, unlike what happens with many other webmail providers. Only on the off-site backups (which are fully encrypted, of course) a copy will remain for the maximum retention period of three days. Your Account will be stored for as long as our Agreement remains in force. When an Agreement is fully terminated, all data contained in the Account, including all emails, will be deleted permanently.*

As well as their policy in dealing with requests:

> *We will not comply with requests from any authorities other than Dutch authorities. If we receive a request from any foreign government, we will refuse to comply and will instead refer the requestor to place a formal request to the Dutch authorities for mutual assistance.*

> *StartMail will never cooperate with any voluntary surveillance programs. Under the strong current laws that protect the right to privacy in Europe, European governments cannot legally force service providers like StartMail to implement a blanket spying program on their users. Should that ever change,* ***we will use all methods at our disposal to resist.***
>
> *We will not comply with any requests from private third parties to provide information about our Users, unless we would receive a valid Dutch court order to such effect.*

Though it's cool they won't share your stuff with snoops without a valid court order, as well as having a sane deletion policy - let's not get bamboozled here. **Not a word is said about the storage of your E-mail content and metadata**, which is the most important part of a privacy policy - and yet it doesn't exist here. There's one more thing you might want to know about. Since the service is paid, and they don't accept bitcoins, you won't be anonymous. And **they keep payment information for 7 years** - *"We store invoices for 7 years, or whichever period may be prescribed under applicable tax law"*. And, according to Wikipedia, invoices contain personal data, such as your name. Despite a lot of posturing, I can't recommend StartMail as long as they keep us in the dark in terms of the most important information. Also, recall that some time ago, StartPage was bought by a data collecting big corporation (archive) (MozArchive) - and even though they allege that StartMail is a separate entity, you'd be naive to think that stuff won't spill over.

Dismail

UPDATE March 2024: registrations enabled again; require captcha that doesn't seem to load in

Pale Moon.

UPDATE July 2021: registrations now disabled. As I've explained, it's all about money in the end, and these single-person services can't be relied on.

> *It's no secret that providing dismail services is very time consuming. This is 3 hours every day for the last 6 years. Sometimes less, sometimes much more. With family, job and other commitments, this means very long days. Unfortunately, the day has a limited number of hours and so it comes (among other important things) that I have hundreds of unanswered requests and questions in my inbox, I just don't have enough time to answer them all in a reasonable amount of time. This is frustrating for you and for me.*
>
> *When will you reopen the registration?*
>
> *If I won the lottery, maybe.*

Requires sending them an XMPP message before you get access to your E-mail account, but the activation appears automatic. Signing up requires no personal information and is possible through TOR (no onion domains). Supports mail clients. The English privacy policy (archive) (MozArchive) has been deprecated by the German one (archive) (MozArchive) that a member of our chat graciously translated for me. All your mail content, attachments, subjects, senders, recipients, message sizes, the last login date, and IP addresses are stored for 7 days minimum. This is way worse than what the earlier version had and makes Dismail pretty much a violator. The ToS (archive) (MozArchive) is also quite restrictive:

> *the sending of messages with the aim of harming or destroying, violate privacy, infringe*

> *the intellectual property, to issue statements offensive, fraudulent, obscene, racist, xenophobic, discriminatory, or any other form of content prohibited by law.*

In other words, pretty much the SJW favorite victimization issue list. Plus no porn, no copyright violations, no *"abuse of others"* and no *"software for the circumvention of copy protection"* which could include even torrent clients by a loose definition. Apparently only one guy runs Dismail, so it could go down if he gets bored. Not that you'd want to use it when there are much better alternatives. Though - in a pinch - it does allow TOR signup without personal data or ReCaptcha as well as mail client support, so it's decent, at least.

Migadu

A friend has made me aware of this one and called it his favorite, but I don't like it for a few reasons:

- **It's paid** - that alone does not kill it, but free should be prefered
- **You must pay for the whole year** ($19) upfront if you want the Micro plan, which is the cheapest. The other plans are extremely expensive and I'd say, not worth it for a simple E-mail provider.
- **You must contact them personally** if you want to pay with Bitcoin, but at least they do support the option
- **They don't provide a domain**, so you must buy your own which is an additional cost
- **The Micro plan allows only 20 outgoing messages** per day, which is kind of low. To be honest, I never reach it with my own E-mail usage, but depending on what you do, 20 might easily be too little.

- **They require giving them your real name to sign up**
- **They require an existing E-mail account**; temporary ones are banned
- **They store your outgoing messages** for up to 30 days
- **They store your IP addresses** but claim they are *“anonymized”* - you are not informed of how that is accomplished, however.
- **Inventory data is stored for up to two years**, and possibly more if some unspecified legal stuff applies.

So, Migadu is a paid provider that needs a domain and whose privacy is not that great. At least they allow Bitcoin payments and support mail clients. Overall, I'm not impressed and would much rather go for Disroot, RiseUp or Posteo / ~~CounterMail~~ if money is not an issue.

📪 Cock.li 📪

UPDATE January 2024: *“Cock.li is back open for public registration! New accounts receive mail instantly, but are blocked from sending mail until you allow you browser to complete a proof-of-work challenge that only takes a few minutes.”*

UPDATE May 2021: registrations closed, soon to be invite-only. I guess an inferior RiseUp, then? Or superior, if you really hate *the commies*.

Sounds good at first glance - supports mail clients (though **Claws Mail could not automatically detect the settings** and required manual configuration), does not ask for personal information, *“allows registration and usage using TOR and other privacy services,”* and *“is run by "some dude", not a business”*. So is this **the** service to use? For that, we will have to see what data does

it collect, as usual:

> *IMAP and SMTP logs include: When an E-mail is sent, the username, destination e-mail address, and information about the connection (like IP address, quota information) When you connect to IMAP, what IP address and username (if any) you are logging in with, and if that login was successful*

These, according to cock.li's privacy policy (archive) (MozArchive), are stored for 48 to 72 hours. When you visit their website, cock.li stores this information: *"HTTP access logs containing your IP address, user agent, and type/location of your requests"*. They say it's not related to your account, but it would be trivial to connect them.

Cock.li's privacy policy is a little unclear on that point, but it seems that you can delete all your data manually - aside from registration information - and it will be gone immediately. Removing the latter requires **erasing your account**, but even then, that data will be kept for 30 days.

Cock.li has to be commended on its honesty. Privacy policy and ToS are short and straight to the point. It admits it can read your mail and that it cooperates fully with law enforcement; transparency and donation reports are also available. There's one other thing you might want to know about though...

https://arstechnica.com/tech-policy/2015/12/cock-li-e-mail-server-seized-by-german-authorities-admin-announces/ (archive) (MozArchive) .

> *"That means that SSL keys and private keys and full mail content of all 64,500 of my*

users, as well as hashed passwords, registration time, and the last seven days of logs were all confiscated and now are in the hands of German authorities,

Yeah...I mean, could this have gone any worse? The victims of this breach were probably wishing they never cared about this "privacy" stuff and still kept using Gmail, haha. Also, forget about having a normal domain name with this guy - they are all shitty jokes about cocks, rape, memes like blazeit and others you'd rather not show to most people. Another really significant issue is **how often the cock.li domain is blocked** on various sites. With that in mind, I cannot anymore say that this is a good choice at all. It does at least have an onion domain at http://mail.cockmailwwfvrtqj.onion/; this, however, does not prevent them from reading your mail or storing the metadata.

Paranoid

Alleges itself to be extremely privacy based, with quotes such as *"Our mission is to return the feeling of privacy back to people."* and *"Return the privacy to day-to-day email communication and make it as popular as possible."* However, **the service has no privacy policy**, so you can't know what do they actually store. They say that they are *"PROBABLY THE ONLY OPENPGP-ENCRYPTED EMAIL BOX"*, but that isn't really true - even the dreaded ProtonMail and MailFence have that (though the implementaion is worse). Supports mail clients and has an onion domain. Here's the big thing though - Paranoid **requires an invite**, which I tried to get a few days ago. First, it told me that my cock.li mail is "disposable" and won't be accepted. Then I signed up with real disroot account and - though the message about the disposable services didn't appear - I still didn't get a reply in 5 or so days. One of my contacts says his friends sent requests **months ago** that are still not accepted. Thus, regardless of

its privacy, Paranoid appears to be pretty useless.

UPDATE February 2020: The above is what I wrote very long ago. Then, the service went down shortly after so I assumed it's dead. Now it's back and one of my contacts was impressed with it, so I investigated again. **Everything I wrote above is still true**, except I also tried to sign up with my RiseUp E-mail alias, and got rejected for using a "disposable address". However, the contact managed to get through the process so we did some tests. Paranoid claims that:

> *If a sender can't encrypt the eMail which will be sent to your @PARANOID box - we will encrypt it for you using your public key - the only key we store.*

This is true. Any E-mail sent to a Paranoid address will be encrypted by them with your public key (which you will have to generate and upload). However, since the encryption is done by Paranoid - they (as well as the sender's server) **can still see the contents**; and as they have no privacy policy, we don't know what they do with that. Let's check out another quote:

> *@2048.email & @4096.email aliases can receive encrypted eMails only. We will check for you, if an eMail, which has been sent to you, is encrypted.*

Unless we've understood it wrong - **the above is false**. I've sent an unencrypted E-mail to both of those addresses, and my friend received them, where according to the claim - they should have been "bounced" back to me. I did, however, get a message implying that the unencrypted E-mails did not go through:

> *Dear owner of the email address email_redacted@some.domain, recently you've sent an email to the email_redacted@4096.email which is in the 4096.email domain provided by*

> *Paranoid.EMAIL service. This user does not accept unencrypted emails. Please encrypt email using PGP and send it again. If you do not know the key you can ask using this email email_redacted@paranoid.email To avoid seeing this 'bounce' message again in the future you can either start sending OpenPGP-encrypted eMail messages to the recipient (if you've already familiar with OpenPGP/GnuPG) or alternatively, you can become an early bird tester of our brand new encrypted eMail service...*

Of course, even if he did not receive them, they would still have traveled unencrypted from my machine, through my provider, ending at *Paranoid* (with many other points inbetween). So, him not being able to read them wouldn't provide any security. What does the "bouncing" accomplish, then? It might possibly (in some alternate world...) get the other guy to encrypt using PGP - however, to have real end-to-end encryption, that person **would also have to generate his own keys**, which - for the vast majority of people - is insurmountable. Also remember that the above applies **only to the 4096 and 2048 aliases** - you can still give the regular *"paranoid.email"* one to avoid the bounce.

The above, however, is still the best implementation of PGP you can have without PGP proper. At least they are not doing decryption in the browser, or worse - storing your private key like ProtonMail. In fact, they are specifically warning against those approaches (MozArchive). Not only is there **no security or other disadvantages** in what Paranoid is doing, some benefits even exist. The messages you receive will be encrypted for at least a part of the journey without the other person's involvement (again, you must upload your public PGP key), and you might "convert" a few people to real end-to-end encryption in PGP (at the cost of annoying some others).

Despite all the above, Paranoid is actually a **pretty good email service**. It sucks that they

consider so many real E-mail addresses as "disposable", but what can you do? If you get past that, you can sign up for free through anonymizers and without providing any personal data - which is already miles above what many others are doing. They also **realize the perils of webmail and don't even provide it** - therefore, you must use them through a mail client. An onion domain is available as well. The biggest problems (aside from the ones with signing up) are not having a privacy policy and making some weird statements on their main page - however, language is very clearly a barrier here. In summary, I can't recommend this one with the registration issues as well as not having a privacy policy - but it is better than most others allegedly private ones that are listed here.

Cotse

A reader has made me aware of this one, and I think it's particularly good so I'm whipping out this review immediately. **UPDATE**: sorry, it seems I have missed important information - the service is **worse than I thought**. Read on:

First of all, their website is refreshingly simple and easy to navigate. Compare to something like Proton or Runbox with their huge fonts, random space inbetween, and deceptive slogans. Or Criptext, which doesn't even display anything without enabling JavaScript (*Cotse*'s site has no scripts).

But let's move on to the stuff that actually matters, which is the service's inner workings. Cotse **is a paid provider**, and you must pay for half a year outright, which comes out to about 4 USD per month (similar to CounterMail). They **do not accept bitcoin** - but do cash by mail (archive) (MozArchive):

> *We do also accept checks, money orders, and cash sent by regular mail*

This is the preferred option from an anonymity perspective. The privacy policy (archive) (MozArchive) nicely tells advertisers to fuck off, and also admits they will fight any attempts to receive information. But what do they actually log?

And this is where Cotse's cracks begin to show. Their logging page (archive) (MozArchive) starts with some information about how logging works and why an E-mail service can't operate without any. Cotse even nicely shows you what actual SMTP logs look like:

> *Nov 18 13:25:23 www mta[12345]: AUTH=server, relay=domain.com [127.0.0.1] (may be forged), authid = account, mech=<type auth= "auth" of= "of"> Nov 18 13:25:23 www mta[12345]: XXXmpe12345: from=, size=405, class = 0, nrcpts=1, msgid = <messageid>, proto=ESMTP, daemon=TLSMTA, relay=domain.com [127.0.0.1] (may be forged) Nov 18 13:25:23 www mta[12346]: XXXmpe12345: to=, delay=00:00:00, xdelay=00:00:00, mailer=esmtp, pri=12345, relay=receivingmachine.domain.com. [receivingmachineIP], dsn=2.0.0, stat=Sent (iAIIPOAb089975 Message accepted for delivery)</messageid></type>*

These appear to indicate that the customer **IP address is not stored** - as in, it's set to 127.0.0.1 (the localhost) and unable to identify you. Unfortunately, on another page (archive) (MozArchive) , they admit that to be wrong:

> *- Login IP addresses and associated time stamps. (only available from last five days.)*

This is the part that I've missed during the earlier review (a reminder to **always dig deep**!), and

it kind of dooms Cotse. It's too bad, because I really thought I could compliment them on their honesty, but I can't now in good conscience (they're better than most in that department, though). The service is still good, but cannot now compare to the ones which do not keep your IP. Cotse **does not store the contents of your messages**:

> *None of our logs record the datastream, as in contents of the email*

There are no backups, either:

> *Automatic backups can compromise your privacy because there is a backup to seize of something you deleted. For this reason we do not back up any user data, neither e-mail nor web space.*

Which is actually the only privacy respecting option; thanks to this, you're ensured that after five days, no logs are left. Still, five days is kind of long compared to other services (e.g Disroot) which can manage with 24 hours somehow; but it's still better than what almost everyone out there is doing. E-mail clients are of course supported (if they weren't, I wouldn't even bother reviewing the service) - and you can download the E-mails using POP3, which will also delete them from the server. Lots of domains are available, including using your own. There are many spam filtering options (archive) (MozArchive) , but you're not required to use any of them so there's no worry of E-mails being randomly rejected (like what Disroot does sometimes). Cotse also has an alias feature similar to RiseUp's:

> *We give you unlimited addresses in twenty domains plus unlimited addresses in any of your own custom registered domains. This is so you can give each place that requests an e-mail address its own custom address.*

However, it **does not work as well**, because it reveals your real account (archive) (MozArchive) in the alias:

> *For much of your email needs, you can create unlimited aliases of the form (alias)@(yourname).cotse.net, without the parentheses.*

So, if someone visits Cotse's site and learns how the alias feature works, they can figure out that your main E-mail address is *"yourname@cotse.net"*. Still, the feature should work well against bots. There's no Bible of banned things (archive) (MozArchive):

> *We have a zero tolerance for fraud, spam, harassment, theft, terroristic threats, cracking or DoS attacking other servers, or child porn.*

This is less than what any other provider has. Anyway, summarizing: Cotse is a pretty expensive service with good quality. The main flaws are that it **stores your IP address** for five days and doesn't accept Bitcoin payments. Cotse has been around since 1999 so there's little danger of it going down. It's a good choice if you don't trust *the commies* - just remember to **always use anonymizers** when using it!

CounterMail

UPDATE April 2022: Countermail is CUCKFLARED NOW. Holy shit! Ignore everything I wrote below, get some cockroach repellant, and RUN! **UPDATE November 2022**: apparently the mail itself **does not go through CF** - only the website - according to a reply from Countermail. Still, beware of any service that touches CF.

My old review of this one was kind of lackluster, so let me try again. First of all, CounterMail now **requires an invite code** to register - but unlike RiseUp, it's also a **paid service**. The price is 29 USD for six months - and that's the least you can pay for; Bitcoin is fortunately accepted. JavaScript must be enabled for registration; there are no captchas or anonymizer blocking. There is a free tier that's pretty much useless, since it doesn't even support mail clients and has a bunch of restrictions in terms of E-mail recipients.

Upon registration, CounterMail will generate a pair of PGP keys, which will be used to encrypt all incoming and outgoing E-mail if possible. If your recipient is another CounterMail user, messages will be automatically encrypted for the whole journey. Otherwise, they'll be sent in the clear from your recipient until hitting CounterMail's servers, then encrypted back to you. The problem with all of that is - of course - that **CounterMail stores your private key** on their server. They allege it's only stored encrypted with your password, but they could easily swipe that since you must type it to log in each time. Still, even that kind of encryption is better than plaintext - since at least middlemen can't access your messages, even if you do not trust CounterMail. But nothing compares to PGP that you manage locally, as long as your recipient is able to do so as well. **UPDATE July 2021**: it seems that now you can delete the private key (MozArchive) from their servers and even use your own (MozArchive). This is the best of both worlds - newbies can rely on CounterMail's encryption while pros roll their own.

Privacy policy (archive) (MozArchive) says that **IP addresses are not stored**, ~~but keeps you in the dark in regards to any other information~~. **UPDATE July 2021**: a reader informed me they've updated their privacy policy recently, and the most important addition is this:

> *We do not collect any data from our users, the only time we store some data is the first 14 days of your payment date, after 14 days, we remove most sensitive information and only*

> *store the data that is needed for the accounting, such as the product you bought, the amount, the payment method, the date and the country. So after 14 days: no Name, no Address, no State, no Phone, no Card numbers and no Secondary email*

If we take this at face value, **CounterMail becomes the provider that stores probably the least amount of data** out of them all. The only way you could make it better is to tell us whether our E-mails (or their metadata) are stored after downloading by mail client and / or deletion through webmail - and if so, for how long. Mail clients are supported in the paid tier (which I didn't bother paying for, and so couldn't test). For an additional 15$, you get the option to use your own domain. There is an alias feature that actually works properly - as in, doesn't reveal your real account in the alias - something which only RiseUp has managed to do otherwise. There are a bunch of webmail-only features that I don't care about, because well...they are webmail only. The ToS (archive) (MozArchive) is pretty lax, only forbidding stuff that's illegal in Sweden, as well as spam. To be honest, I have trouble rating this service. They seem to really care about privacy and security. The price is also pretty high - more than four times the amount of Posteo, for example. Overall, with the newest privacy policy change, CounterMail becomes one of the best providers out there. I think the only real flaw now is the price, but at least the product is worth it.

Fedora Email

UPDATE Jan 2024: *"User registration is disabled"*

Someone just notified me about this one, and well, I thought I might squeeze it inbetween my more important work, so let's go. You can make an account through TOR and without enabling

JavaScript, but cookies seem to be required. The page tries to load a recaptcha but it's not being used for anything, it seems. You can login to the webmail without JS, but much functionality is JS-dependent - like even reading the mail, or changing settings. Of course, in the end we want to handle our mail with our separate mail clients, and Fedora **does support that option**; sending and receiving both work properly. Fedora allows creating aliases through the web interface, but they reveal the original identity in the headers. This provider also **leaks your IP address** to your contacts (with the header *X-Originating-IP*), so you better **use it only through anonymizers**! You can enable 2FA, as well as GPG encrypted storage of mail (this would protect against hackers reading your messages, but not against Fedora itself), but I'm not going to test that. So, technically this provider seems pretty good; any other problems?

Well, it requires a real name for signing up, and the ToS (archive) (MozArchive) prohibits giving fake data:

> *When you create an account with us, you must provide us information that is accurate, complete, and current at all times. Failure to do so constitutes a breach of the Terms, which may result in immediate termination of your account on our Service.*

Zero idea how well they check up on this, and I won't get to learn, as I don't intend to use this provider. The entire ToS is auto-generated - *"Terms and Conditions for Fedora Email based on the T&C example from TermsFeed."* - so the administration doesn't seem to be taking anything too seriously. There is no privacy policy, either; the only thing you learn about their data handling is this tidbit from the main page:

> *What is this?*
> *An email server that doesn't sell your data.*

Amazing. It might still give it away for free, though. And you never get told what is stored and for how long. Who actually knows who's running this? It's not listed anywhere. Usability-wise, Fedora seems adequate - but there are some suspicions because of the lazy ToS, no privacy policy, and shadowy administration (assuming it's run by one guy, it might just go the way of dismail soon, so I don't recommend relying on it long term). However - if all you need is a provider that doesn't discriminate against TOR, is free, and works with E-mail clients without hassle - then Fedora should fit the bill.

Posteo

Their privacy policy (archive) (MozArchive) starts off very promising:

> *we strictly do not save any IP addresses that could be traced back to customers. [...] This was independently confirmed in an audit report by the German Federal Commissioner for Data Protection.*

The audit is in German so I can't confirm what was actually checked, however it's nice that they bothered to do it.

> *We also do not collect or save your IP address if you use an external client to retrieve your emails via IMAP or POP3 or to transmit messages via SMTP to be delivered by us.*

So, if you use a mail client, your IP is not stored at all. How about the mail contents? Posteo **doesn't seem to directly say what is stored and for how long**, besides the fact that you can wipe it:

> *When you delete content data, it's deleted immediately. If the data has been backed up in one of our daily security backups, it will remain there for an additional 7 days until it is completely deleted.*

So you can delete your mail anytime, and it's gone except for the backup. Not bad; you can encrypt the backup as well:

> *Additionally, we offer the possibility to encrypt all emails, notes, contacts and calendar entries that are saved at Posteo individually with the password of the account (AES-encryption).*

Posteo **is a paid service** (1 EUR per month), though it alleges that the payment data is anonymized (as in, not connected to your account); you can read more about this here (archive) (MozArchive). However it is unclear what is actually saved - on one hand, they say that *"Despite the change in the law, we still do not save any of our customers' user information"*; and on the other - *"For PayPal payments: The time and date of a payment, the amount,* ***and the name of the payer****"*. The data is stored for 10 years; they say it is not connected to the user's account, but you will have to take their word for it (**UPDATE April 2023**: a German native speaker just told me: *"I read through the audit documents they provide, the data protection official says the data is properly detached"*). Cash payment by letter is also available and apparently, it's possible to do that **without giving personal data to the post office**. Nice! Means we have a truly anonymous way to sign up for Posteo (if you're worried about CCTV or whatever, send a friend). Still, they should get with the times and accept crypto already...Anyway - since I did this for Disroot, RiseUp and Autistici - let's now check out what does Posteo's ToS (MozArchive) prohibit:

> *5.3 The customer will not use the email service to send out advertisements for commercial purposes by email or to send standardised emails to a multitude of recipients.*

So you can't advertise your commercial service, despite Posteo itself being paid for and not following anti-capitalist politics. Weird. You also can't *“break German laws”* and *“break regulations regarding protection of children”*. Pretty mild, I guess.

Since June 2019, the German laws have changed so that **targeted surveillance by the government is now unlawful** (maybe we should be speaking about *“German privacy laws”* instead of *“Swiss privacy laws”*?). Quoting from Posteo's transparency report (MozArchive):

> *At the present time, there is no longer any legal basis for TKÜ (surveillance of an account for a specified time period); Posteo is therefore no longer allowed to and will not implement such orders.*

No tracking shit on their website, unlike StartMail. No IP storage, e-mail deleted immediately upon your action and only stored in a backup encrypted with your password. No personal information collected ever; payment data (allegedly) anonymized as well, so even when the government comes knocking, they get nothing. Two aliases are available upon signing up, and you can buy more. You can't use custom domains with Posteo and it also does not have an onion domain available. Posteo **is powered by renewable energy sources**! So you're protecting the environment with this provider, as well. Taking everything into account, this service is one of the best out there, though it does have a few flaws.

Morke

This provider has some unique properties. Namely, the most "no bullshit" way of signing up that I've ever seen. Well, the only one is being onion-only, which I guess will keep away 90% of people. But since you are here, you surely won't get discouraged by things like that. Otherwise, you just type a login, password, and solve a simple captcha (that I'm positive bots have long since fucked, but whatever - it works for us). Annoyingly, the password policy **prevents special characters**, but it's not that violating - I'm sure you can come up with a good one that only has numbers and letters. If you're getting the "wrong user or pass" error during login, it's either that you didn't type the domain right (for some reason it's still *yourname@morke.org*, and not the onion!), or failed to enable cookies (JavaScript is not required). There is **no privacy policy** at all, so just assume they are storing everything forever - though it's not necessarily the case, but still. You could use PGP to partially prevent this danger (hiding the message content), but Morke also makes that hard to use, since you can't just slap this account onto your mail client and add automatic PGP support there, as **it's sadly webmail only** (SquirrelMail). Their onion also seems to go down quite often (like at the moment of writing). Because of all of this, Morke is really unwieldy for actual regular communication. So why it's so high in the rankings?

Well, it has one use case for which it is absolutely perfect - namely **receiving confirmation mail** without connecting them to your other identities. And I know, that providers like Disroot and (especially, due to aliases) RiseUp work decently well for it too, but what if you want to separate certain activities? What if you don't want to risk your main email account for...something that might be declared suspicious and compromise your entire internet existence? Well, that's where Morke comes in, and that is why it is so high. Better take advantage of it before it disappears, like dismail (though a little more "bullshit" there) and dnmx (which got raided (archive) (MozArchive)) did before. These "unknown internet

shadow"-run services don't tend to last long - whether due to the raid, not being profitable, or just lost interest. You know, despite the initial excitement, it can take quite some effort to set them up and maintain them. Morke's first webarchive page seems to date to the late 2021, so it's already been around for over 3 years. Cock.li lasted longer but had quite the dedicated userbase (that also was donating a lot of money); dnmx didn't last long at all. Last time I checked pissmail was dead but it seems to be back now; yet the downtime exposes the unreliability of such services regardless. And when Morke disappears, we'll again be left on ice for "simple" ways to sign up for things. Then you'll see just how painful it is to lose this ability, as I have learned only a few days ago. This justifies the ranking right before Disroot and RiseUp that are more fit for regular communication.

Disroot

UPDATED March 2023. I went on to confirm that all the policies are still the same, and **they are** - just with some wording changes. Also took the time to improve the descriptions, remove clutter, etc.

Starts off with some nice quotes. From the front page:

> *Disroot is a platform providing online services based on principles of freedom, privacy, federation and decentralization. **No tracking, no ads, no profiling, no data mining!*

The About page (MozArchive):

> *In the last few decades information has become very valuable and more and more easy to collect and process. We are accustomed to being analyzed, blindly accepting terms and*

conditions for "our own good", trusting authorities and multi-billion dollar companies to protect our interest, while all along we are the product in their 'people farms'.

Many networks use your data to make money by analyzing your interactions and using this information to advertise things to you. Disroot doesn't use your data for any purpose other than allowing you to connect and use the service.

Disroot aims to change the way people are used to interact on the web. We want to encourage and show them not only that there are open and ethical alternatives

And the mission statement (archive) (MozArchive):

The once decentralized, democratic and free internet, has been dominated by a handful of technology giants, promoting concentration in monopolies, more government control and more restrictive regulations. Everything that, in our opinion, opposes and destroys the true essence of this wonderful tool.

Our motto is "The less we know about our users, the better". We implement data encryption whenever possible to ensure that obtaining user data by unauthorized third parties is as difficult as possible and we maintain only the minimum of user logs or data that are essential for the service performance.

We chose a working approach in which users (from now on referred to as Disrooters) are the most valuable part and the main beneficiaries of the project

So, we get the impression that Disroot dislikes what the Internet has become - a place where

we're data-mined, controlled, dependent on powerful entities that don't have our interests in mind. Sounds great; but as usual - what's most important is the confirmation of the ideas espoused above - after all, Mozilla, for example, says the same things. So let's check out their Privacy policy (MozArchive). Starting with the E-mail specific one:

> *Server logs, which store information such as, but not limited to, your username and your IP address, from and to email addresses, IP addresses of servers the emails come in or go out to, are stored for a period of 24 hours after which they are deleted from the server. No backup of log files is created.*

So, all logs are wiped every day. There's also no backup. Very well, can't do much better than this.

> *All emails, unless encrypted by the user (with GnuPG/PGP, for example) are stored unencrypted on our servers.*

If you worry about this, realize that you can just download your E-mails with your client through the POP3 protocol, and then they won't be stored at all after that. You can also use PGP as they say. Disroot also uses disk encryption. This is it for the E-mail specific policy, so let's check out the general one:

> *We do not sell your data to any third party.*
>
> *We do not share your data to any third party [...]*
>
> *We have no advertisements or business relationships with advertisers.*

We store all data in our own servers, located in a data center in the Netherlands.

In short, **your data stays at Disroot**. If you scroll back to the other providers, you will see that barely anyone else - if anyone at all - follows this policy. Let's now check out their Terms of service (archive) (MozArchive). The relevant parts are these:

2. Contributing to the discrimination, harassment or harm against any individual or group. That includes the spread of hate and bigotry through racism, ethnophobia, antisemitism, sexism, homophobia and other forms of discriminatory behavior.

3. Contributing to the abuse of others by distributing material where the production process created violence or sexual assault against persons or animals.

Shortly, **no violence, abuse, or discrimination of others** (the latter could be worrying depending on how strict of an interpretation is taken, but whatever). Using Disroot for commercial activities is also not allowed:

Because of this structure we see using Disroot services for commercial purposes as abuse of the service and it will be treated as such.

Knowing what I know now, this rule is understandable to me - but will bother a lot of people, for sure. If you want an E-mail for your business, I'd suggest another provider. Even then, Disroot will not immediately kill your account when such an activity is detected:

5. Using Disroot services for any other commercial activity will be examined per case and the decision on terminating such accounts will be based upon communication with

the account holder and the type of the activities in question.

This ToS is still more lenient than almost any ToS out there. Disroot allows signing up through a VPN or the TOR network, including an onion domain. Mail clients are supported - but you can use the RainLoop webmail as well, which supports PGP encryption - but they tell you not to rely on it and instead encrypt your shit locally (as I've been saying all throughout this report).

Nevertheless, we encourage you to always be cautious when using email communication, and to make use of GPG encryption to ensure your correspondence is safer.

Signing up for Disroot requires filling a "Your Story" section (**UPDATE**: this is now answering a *"What is the first thing you think about when you wake up in the morning?"* question). Earlier, they've used ReCaptcha to deal with the spam problems they had, but - due to privacy reasons - dumped it and had to come up with something else, so there it is. If you do so, you also get access to some other services, including a forum, where you can read that Disroot is in for the long haul (archive) (MozArchive):

So as far as I'm concern disroot isn't going anywhere. It is my primary email address, xmpp account and d account.*

I think we have something, big corporations don't. We believe in what we do, and the change of current status-quo. Going back to the roots, to how the internet used to be.

We started disroot with "long run" in mind. From my side I can tell you, disroot is my baby and I believe in it's success (or however you want to call it). You don't kill your babies.

The admin also claims the service is not activist exclusive (archive) (MozArchive) - unlike RiseUp or Autistici:

> *I dont know where did you get the information that we are somehow for activist exlcusive. Nowhere on our website, neither in our Mission statement we say anything about it.*

Me and a chatroom member also did tests with him sending E-mail to my account from some rarely used providers (such as Paranoid or Onion Mail), and **Disroot blocks them**, forcing the other person to resend. This is a way of spam filtering which **does result in 99% of spam being blocked without your input** - but the few false positives are annoying, for sure. To inspect the rejected spam mails anyway, you can check the webmail's *"Junk"* folder.

In summary - logs stored only for 24h, no personal data required for registration, VPN / TOR usage allowed. So, privacy is very good and they mostly **did end up confirming their mission statement** - unlike Mozilla. The issues with Disroot include: blocking unknown providers and a somewhat restrictive ToS (no discrimination or violence, no commercial usage) - however, still much less so than almost all the others. You also have to pay for aliases. Along with RiseUp, Disroot is still the best free option out there.

Elude (DEAD)

Curiously, cookies are required just to view the site. Registration possible only through TOR (**now v3**); no personal data is needed - only solving a ~~text-based captcha (which often appears to ignore correct solutions, for some reason)~~ really hard picture captcha. Front page says *"Elude mail is free. We will never require you to pay to use our email service."* However, **mail client**

usage requires a donation (1 USD per month, in Bitcoin or Monero) and the free tier also needs the user to answer the question *"To prove you are human, please describe why privacy is important to you?"*. So it's effectively a paid service since mail clients are such an essential feature. Good privacy policy, not logging IPs or browser data; no third party sharing; FDE enabled. The only thing they store are the registration date, last login month as well as the sender and recipient metadata (the last one is deleted after 24h). ToS is lifted verbatim from RiseUp:

> *You may not engage in the following activities through the services provided by Elude:*
>
> - *Harassing or abusing others by engaging in threats, stalking, or sending spam.*
> - *Misuse of services by distributing viruses or malware, engaging in a denial of service, or attempting to gain unauthorized access to any computer system, including this one.*
> - *Contributing to the abuse of others by distributing material where the production process created violence or sexual assault against anyone.*

This is still very mild compared to all other providers - most of which have a Bible of requirements to follow. Compared to RiseUp below, allegiance to anarchist / "commie" ideology is not required. All in all, Elude is a very good choice assuming you consider it a paid service. Onion access, no personal data, first-party captcha (but hard to solve), great privacy, decent ToS and 10 aliases for the first paid tier (1 USD / mo). The copied ToS looks kind of suspicious, but whatever. Also, we don't know who made the service and if they're going to stick around. Keep in mind I did not truly test this provider because I didn't pay (but might eventually), so I don't even know anything about possible downtimes etc. Still, from what I can discern, Elude is a great option, second maybe only to the below.

✦ RiseUp ✦

> *The Riseup Collective is an autonomous body based in Seattle with collective members world wide. Our purpose is to aid in the creation of a free society, a world with freedom from want and freedom of expression, a world without oppression or hierarchy, where power is shared equally. We do this by providing communication and computer resources to allies engaged in struggles against capitalism and other forms of oppression.*
>
> *We work to create revolution and a free society in the here and now by building alternative communication infrastructure designed to oppose and replace the dominant system.*
>
> *We promote social ownership and democratic control over information, ideas, technology, and the means of communication*

This is exactly the kind of stuff I've spoke about in the Avoiding "The Botnet" - impossible? article. If RiseUp realizes the source of the "botnet" and the need to control the infrastructure, then surely their service does not spy on you. Let's check it out (archive) (MozArchive) though, to be sure:

> *No IP addresses of any user for any service are retained.*

Good, the most important one is out of the way.

> *Your web browser communicates uniquely identifying information to all web servers it visits [...] We do not retain any of this information.*

So, user agents and stuff like that isn't collected. So what do they actually store?

> *we keep a log of the “from” or “to” information for every message relayed. These logs are purged on a daily basis*

So the sender and recipient metadata is stored but only for 24 hours at most, apparently for the prevention of spam. But then comes this:

> *Anonymous, aggregated information that cannot be linked back to an individual user may be made available to experienced researchers for the sole purpose of developing better systems for anonymous and secure communication. For example, we may aggregate information on how many messages a typical user sends and receives, and with what frequency.*

If I have criticized Mozilla and DDG for the same thing, I can't let it slide here. Though, of course, it's mild compared to what everyone else is doing.

> *You may choose to delete your riseup.net account at any time. Doing so will destroy all the data we retain that is associated with your account.*

Okay, so regardless of what is stored, if you delete your account - it's gone for good. The only sane policy that unfortunately isn't used by most other providers.

The more important things, though, are said in their RiseUp and Government (archive) (MozArchive) section:

> *We will do everything in our power to protect the data of social movements and activists, short of extended incarceration. We would rather pull the plug than submit to repressive surveillance by our government, or any government.*
>
> *We have fought and won every time anyone has tried to get us to give up information. We have never turned over any user data to any third party, fourth party, fifth party or any party.*
>
> *We would not consent to the installation of any external hardware or software on our network and would end the organization rather than install any.*

So they admit they will fight the government and would rather die than surrender. What other provider would do that? However, the claim that they've never turned over data is false:

> *After exhausting our legal options, Riseup recently chose to comply with two sealed warrants from the FBI, rather than facing contempt of court (which would have resulted in jail time for Riseup birds and/or termination of the Riseup organization). The first concerned the public contact address for an international DDoS extortion ring. The second concerned an account using ransomware to extort money from people.*

Even though this might seem justified by the apparent evil of the actions, it **opens a can of worms** that I'm not sure should be opened. I mean, the legal system itself is a massive oppressor and we shouldn't ally with it just because it happens to do something we like once in a blue moon. After this fiasco, RiseUp has taken steps to further increase privacy - they implemented automatic encryption of mail using your password (similar to Posteo):

> *Additionally, as of March 2017, the storage for all new accounts is personally encrypted. Riseup is unable to read any of the stored content for these accounts. Any user with an account created prior to March 2017 may opt-in to personally encrypted storage.*

You can read more about this here (MozArchive). There is also disk encryption - so you're still protected against the government better than from any other service. And let's be real here - in RiseUp's 21 year long history (as of the time of writing), such a situation has (AFAIK) **only happened once** - while providers like Proton have given away data **hundreds of times**. RiseUp will remove your account for engaging in these activities:

> - *Harassing and abusing others by engaging in threats, stalking, or sending spam.*
> - *Misuse of services by distributing viruses or malware, engaging in a denial of service attack, or attempting to gain unauthorized access to any computer system, including this one.*
> - *Contributing to the abuse of others by distributing material where the production process created violence or sexual assault against persons.*

Pretty mild compared to the litany of things you're not supposed to do that providers like FastMail (archive) or Mailbox.org (archive) have (and **you pay for them**). RiseUp also provides the best E-mail alias feature of all, which is free, does not reveal your real account in the headers, and you can delete the aliases if they aren't useful anymore or have become spammed. Though other providers, such as cock.li or danwin1210, do use the more secure v3 onion domains for XMPP and E-mail, RiseUp is the only one which provides them for the whole suite of services (MozArchive), such as bins, pads, file upload, etc.

All in all, for me this is still **a great E-mail provider** - taking into account the logging policy,

lack of personal data needed for registration, v3 onion addresses, unlimited aliases, mail client support and great reliability (I don't think I've ever had it go down - unlike their XMPP). They also respond to support tickets. The only possible problem would be the FBI fiasco - though, they could not have done much there with the gag order. Remember - **this service is used by thousands of activists** - it has to take privacy and security very seriously. Of course, there is also the focus on anti-racism, anti-"homophobia", etc - but I haven't seen them claim to delete accounts for certain views, unlike Autistici. Other providers - such as FastMail or Mailbox.org - have a litany of things you're not supposed to do in their ToS (ten times longer than RiseUp) - and **you pay for them**. Still, it is a minor issue and since the service has no major ones, I have to mention those. To register, RiseUp requires an invite code from a person who already has an account.

UPDATE September 2024: oh by the way, if you get banned on RiseUp (and maybe even if you simply delete your account), **your previous aliases become available for others**, meaning someone might end up receiving sensitive communication meant for you! This is an insanely big vulnerability. For now, the only way to prevent it - as far as I can see - is to just not get banned. And obviously don't pick alias names that someone else might want to use. If you do end up getting banned, inform your contacts that your addresses are possibly compromised. This really sucks for an otherwise great service.

Temporary e-mail (AirMail and such)

Just for completeness' sake - they're pretty much useless. Blocked everywhere and only stay around for a while, preventing password reset and such. Outclassed by RiseUp's alias feature.

Summary

It is very worrying how many providers pretend to be privacy based but turn out to be anything but - even actively trying to compromise it. No matter, there still exist a few good guys such as RiseUp and Disroot. If you can't or don't want to get into those (perhaps disagreeing with their principles) - the second best option is paying for an Elude / Posteo / ~~CounterMail~~ account. ~~Dismail~~ / Paranoid / Cock are also decent, non-politicized and free services. You should not fully trust any provider, (or any internet service at all). Take this quote from RiseUp to heart: *"Nothing online is 100% secure. If you have something very sensitive to say, do it offline"*. **Encrypt with GPG whenever possible!** That way, you can kind of bypass their censorship / data storage policies even if you're worried about those being used against you. Anyway, if you can't get enough of the E-mail reviews, there are more here.

Why the situation is as it is

E-mail services can be funded in a few ways:

1. By making you pay for an account
2. By collecting and sharing your data, or showing advertisements
3. By paying for it from the maintainers' own pockets
4. By soliciting donations

Option 1 can afford to be private without needing your data - however, that **does not mean it will**. After all, privacy is a big business opportunity now and there are lots of frauds taking advantage (many of them I've analyzed here). Some do exist that do go out of their way to

create a secure, private and functional service - so, use those if you've got the money. Option 2 is obviously undesirable and the reason for this report's existence. Option 3 is extremely rare and doesn't last long (see SigaVPN), so let's move on to Option 4:

For a service to earn donations, **there need to be people willing to give them**. Unfortunately, there are **not enough privacy enthusiasts** for whom that cause is important enough to support monetarily. There is a group of people who do care more about it, though - the so-called "activists", or people *“working on liberatory social change”*. This means the service will be inseparable from the donators' ideology - since it was made by them, for them, anyway. The activists consider it an abuse that the big corpos or governments can spy on their communication or even track their web browsing to show them ads, etc. More importantly, since they use the Internet to talk about their "activism", they **cannot afford** to be watched - because that innocent convo might be used against them during protests, etc. Privacy enthusiasts alone usually do not have an ideology they identify with from which the privacy would follow - they just **don't like being spied on**. They also don't do real-life stuff such as shoplifts, whistleblowing, etc. for which the privacy would be required. We can see, then, why the "activists" care so much more about the issue that they can afford to donate. This is why we don't yet have a service that is free, donation-supported, and without a stated ideology - privacy alone just doesn't move the spirits enough. When the privacy enthusiasts consider the issue more important, these kinds of services will spring up. For now, we're unfortunately dependent on RiseUp, Disroot and some others.

On "privacy-respecting" laws

One of the major ways various privacy frauds advertise themselves. I've pretty much ignored

this issue while rating singular providers, since it's so common and requires a dedicated section to analyze. The claim usually goes something like this:

> *"Our service is hosted in (insert uber-private country of choice), which, instead of (insert non-private country of choice - usually UK or the US), has super-strong privacy laws. Only a valid court order can force us to release your data!"*

You might have already detected the issue while looking at the last sentence. The "super strong privacy laws" claim is based solely on whether a court order is required to release the data. Let's assume they do bring that valid court order - what ends up mattering, then? The data that a service has actually stored, since they can't release what they don't have. **Nothing prevents a service from storing whatever they want despite being positioned in a supposedly privacy-respecting country**. More than that, **many of the countries commonly claimed to be private actually force providers to store certain data**. Examples from specific providers above:

- Dutch law forces StartMail to store your invoices for *"7 years, or whichever period may be prescribed under applicable tax law"*.
- Norway does the same to Runbox but for even longer - *"as financial records must be kept for 5 years according to the Norwegian Bookkeeping Legislation"*
- MailFence (Belgium) keeps deleted account data for a year - *"i.e. the Belgian law imposes 365 days after account closing"*
- And the big fish - ProtonMail's and KolabNow's Switzerland - *"has a legal requirement for six months data retention by the provider."*
- CTemplar's Iceland ~~does the same as above (not 100% sure here though)~~ doesn't seem to do so - but read later to see that's not a perfect protection.

Thanks to the above, we end up with some funny situations like RiseUp (hosted in non-private USA) keeping metadata only for one day compared to KolabNow's six months. But in the end, **the law is your enemy**, not your friend. It imposes the minimum amount of data a provider is required to store, while not preventing them from collecting more if they want to. Being hosted in a country with *"strong privacy laws"* is purely a marketing strategy that mostly seems to arise from US and UK citizens scared of their nations' mass surveillance programs. But other countries - like France or Germany (realistically - probably all of them) - run them as well. More than that, many of them **cooperate with each other**. In 1946, the UK and US formalized an agreement to share intelligence data between themselves; a few years later Australia, Canada and New Zealand joined in (this was called the *"five eyes"*). Eventually the number of eyes increased to 14 as more and more countries became apart of the alliance (with even more "unofficial" members such as Japan or Israel). Edward Snowden's leaked documents revealed that the eyes work closely together to share electronic communication data (abbreviated as *"COMINT"* and *"ELINT"*). For example:

> (TS//SI//NF) NSA's relationship with the FRA, an extremely competent, technically innovative, and trusted Third Party partner, continues to grow. The FRA provided NSA with access to its cable collection in 2011, providing unique collection on high-priority Russian targets such as leadership, internal politics, and energy.

And they admit the operation is becoming more and more effective as time goes on (you can learn more about the history of the "eyes" here (archive) (MozArchive)). What does it mean for the people, though? Choosing a provider from a supposedly privacy-respecting country **does not help** avoid surveillance - many of them are apart of the *"fourteen eyes"* and even if they aren't, they might still cooperate with foreign intelligence. I mean that's exactly what Iceland (non-14 eyes) did during the Silk Road investigation (archive) (MozArchive). They've literally let USA agents in to do whatever they wanted. Therefore, in the end, you shouldn't focus too

much on the country issue (just assume they're all in it together anyway), but instead on the **provider's actual policies, history and trustworthiness**. That plus using encryption, a VPN and good OPSEC should protect you from surveillance way better than falling for red herrings like the service's location.

To put the final nail in the coffin for this idea, we have to come back to the court orders again. To begin - what makes you so sure that a provider will actually require a court order as they state? Remember that ProtonMail has already broken that promise in a case of alleged *“terrorism”*. How much resources do some of the smaller companies have to fight the data requests in court? Do they even have lawyers on board to determine if a court order is valid? SafeMail.nl (based in "private" Netherlands) has admitted they will not fight court orders and just hand over the data. On the other hand, Lavabit (from "non-private" United States) did everything they could to protect their users from surveillance, including trolling the government (archive) (MozArchive). Eventually, they preferred to shut down their service rather than give in to the spies' demands (similar to what RiseUp promises to do today). How many of the providers hosted in supposedly privacy-respecting countries would do the same, instead of just saying "fuck you" to the users and giving up the data? Taking all that into account, I hope we can put the location non-issue to rest...

Back to the front page