Bypassing the privacy chase

Introduction

If you are anything like most people, you have ended up on this site because you've realized your privacy is being violated by governments and big corporations and you've been trying to do something about it. To accomplish that, you've likely traversed recommendation lists like the E-mail report or the Web browser rankings and modified your choices according to them. But is this the right approach?

What is privacy?

The first question we have to ask ourselves is **what actually is privacy** - or else we will fail in our quest to reach it. Simply, privacy is the **default state** of other people not knowing where you are, what you do or think. Though the violators are trying really hard to blur the lines - we're not born with tracking devices under our skins. In fact, our biology is designed with privacy in mind - we're individuals each with our own sets of brains, eyes and ears whose contents are not directly shared with anyone by default. Humans have an ingrained need for privacy (archive):

> *Ralph Adolph and Daniel P. Kennedy, neurologists at the University of Caltech in the United States, discovered that there's a structure in our brain which is responsible for telling us where the limits of our personal space lie. This structure is the amygdala, a small region associated with fear and the survival instinct.*
>
> *This discovery reveals something essential. The brain measures the personal limits of each individual. It's like a personal alarm which tells us when something or someone is bothering us. When something is invading our privacy or violating our integrity until it becomes a threat to our well-being.*
>
> *It reminds us that one of our greatest sources of anxiety is witnessing how we feel more "crowded" every day in every way.*

And so, the *"nothing to hide"* argument totally misses the mark, since privacy is the **biologically necessitated default**. This brings us to our next point:

How do we lose our privacy?

As stated above, we lose it whenever our brain detects another person (or a group of people)

"invading" our personal space. However, **this only works for people** - we've spent over 99% of our time on this Earth in the wild, and that is what our brains are tuned to. There are no computers in the jungle, after all. Civilization has allowed privacy violators to hide behind devices (such as CCTV cameras) and avoid triggering our biological intrusion detection system. Does all this have anything to do with the article title? Sure does:

Privacy in the digital age

Just as privacy in the wild would entail getting away from the people who got inside your personal space - digital privacy works similarly **except the person is replaced by an electronic device**. Though CCTV makes this easy to see, the gadget in question could very well be the computer you use every day, your credit card, printer or even the IoT fridge. We have been so accustomed to a life full of electronics that this simple point eludes us. **There can be no privacy loss with a tech-free life**. Which of course I'm not recommending - only wanted to show the root of privacy issues. Clearly, the amount of data collected while avoiding all electronic devices would be zero - but then we'd lose all the advantages of those. How to balance this?

Technology versus privacy

A privacy newbie usually comes in with the attitude of **replacing his current violators** with privacy-respecting versions. And of course, there are a bunch of providers who are happy to fulfill (or pretend to) that need. You heard your Google Chrome browser spies on you? Mozilla Firefox to the rescue (or not)! Gmail? ProtonMail. Google Maps? Hmm, we're not doing too swell here...Anyway, this same person in 30 years will be asking how to replace Google Parent, Google Cook, Google Home Designer, etc. Is this the right approach? We've established there

can be **no privacy violations** without electronic invaders. Therefore, the way to take control of your privacy seems to be **minimizing device usage**. And so, the right question for a newbie to ask is not *“how do I replace this service?”* but *“do I actually need it?”*

Google Maps has been invented in 2005. Amazon Alexa - in 2014. Siri - 2011. Smartphones - in the 2000s. And yet a lot of people today cannot imagine a life without those. But 20 years ago, we all did fine without them. What has changed? It's obvious technology modifies the way society works (for example, there's a higher requirement for cars or other transportation than a few decades ago), but many of those devices can be easily dumped today - and even the "required" ones can as well with more effort. It is the capitalist focus on shiny new gadgets and the slick marketing which keeps them alive; as well as people's increasing laziness. Real privacy, therefore, has to start with **not being dependent upon the violators** instead of trying to replace, modify or block them.

Things we can give up

- *Google Maps* - paper maps exist or you can just learn the layout of your town. Alternatively, ask the local people if you can't get somewhere.
- *Cloud storage* - really, use USB drives for backups.
- *Home assistants* - a gimmick that isn't needed at all.
- *Digital translation* (such as Google's) - human translators are much higher quality, or you can learn the language yourself.
- *Smartphones* - dumbphones but that still isn't optimal. Unfortunately, most people will have to use a phone occasionally, but you don't have to keep it by yourself at all times.

- *Digital purchases* - Curb your consumption. If you really need something, get it used instead of new and shiny. You can still use the Internet to arrange meetups with people directly. Often, there's higher quality stuff to be found that way instead of a Chinese MP3 player that breaks in a week (this actually happened to me).
- *Any kind of IoT device* - is there really a need to connect your chandelier to the Internet?
- *Social media* - just connect directly with the people you care about (which is not going to be 90% of your social media "friends")
- *Google calendar* - paper calendar? Maybe you have too much stuff going on in your life if you need this.
- *Apple Music* - what is wrong with simply keeping your music on an MP3 player?

Now that we've cut off most of the violators, we can more thoroughly focus on managing the ones we **do actually need** - such as search engines, web browsers (though even this you can curb by avoiding bloated sites and downloading the ones you care about for offline reading) or communicators (hey, there's always carrier pigeons...). So let's end the privacy saga and learn how to choose privacy-respecting services so that you won't have to rely on recommendation lists anymore (which are prone to bribes, fanboyism, groupthink, low quality research, outdated information, etc):

Judging providers

Minimum requirements

Here are the absolute essentials I think any provider should have to even be considered at all:

- *TOR support* - obviously, we don't want to be using some kind of anonymity-hating services that block it.
- *If paid, Bitcoin* (or other cryptocurrency) acceptance - same as above.
- *No personal data required for registration* - this means anything with phone number confirmation is out.
- *Compatibility with established standards* - this can be support for mail clients, OpenSearch, in-band registration (for XMPP), OpenVPN or possibly WireGuard, commonly used encryption (e.g PGP) instead of a special snowflake one, etc.
- *No Cloudflare* (or other MitM) - of course, if all your "encrypted" data is swiped in transit by a known honeypot, nothing else matters.
- *As little downtime as possible* - not so much a privacy-related issue, but in the end, it doesn't matter how good a service is if we can't actually use it.

And with just these minimum requirements, we see that most E-mail providers are disqualified. Many search engines choke on TOR support. Telegram messenger invents its own flawed encryption. Some VPNs lack support for established protocols or are even fully browser based (AKA not real VPNs). Anyway, if you find a provider that checks all the boxes, you might still want to do a deeper investigation:

The privacy policy

This is where a provider tells you what they do with your data. Even the big offenders give that information freely, since (at least theoretically) there are legal repercussions for lying (archive)

(MozArchive). If a provider doesn't have one, I'd consider that a pretty big red flag and probably abandon ship. Same as if it's lacking the necessary information (then it could be storing everything forever, and you'd be none the wiser). **UPDATE:** I don't want to sperg out reviewing providers here again since I've done it enough elsewhere - so check that out for specific analyses. After reading a privacy policy, you should come out knowing at least the basics of what your provider stores and for how long. In particular:

- *IP addresses* - generally, you should bail if these are stored at all (unless with a clause like "in cases of spam" with a 24h or so duration attached)
- *Content data* (messages, E-mails, search queries) - preferably not at all after the recipient gets them (unless chosen by the user for later delivery).
- *System info* - OS, client, settings... - preferably not, but not fatal like the above.
- *Metadata* - who you communicate with and when. No thanks, but rather that than content, I guess? Recall, though, that storing the roster is **necessary for XMPP**.
- *Interaction data* - mouse movements, clicks, referers, ... - pointless tracking shit. Bail.
- *Third party sharing* - a dealbreaker. Assuming data is collected, it should at least not be thrown around to random "partners" (such as advertisers).

Any provider will be on a spectrum between a "no log" policy and storing everything forever and sharing it like it's Christmas. It's up to you to choose the level of tracking you're comfortable with. But to be able to do that, the provider has to actually make that information available in their policy - so bail if they don't. Keep in mind the duration, as well. Some mild tracking might be acceptable if it's only for a short while. Longer than 7 days - though - and it's probably time to bail too. Fortunately, there are at least a few services that do pretty well according to the above criteria - read the E-mail and search engine reports to know more.

History of the provider

Sometimes, a provider supports all the essentials as well as having a good privacy policy, but might still hide **skeletons in their closet**. To fish those out, you need to study the provider's history. Finding red flags can be as easy as visiting the provider's page every so often - for example, you can learn about Autistici changing their privacy policy (archive) (MozArchive) from no logs to 15 day logs or StartPage being bought by an ad company (archive) (MozArchive) - of course they didn't call it that. Sometimes though, it requires fishing out archived pages from 2007 to know the DuckDuckGo owner used to run a data collecting operation (MozArchive) for a few years until selling it to an unethical company and miraculously turning into a privacy guru. From all my experience I can tell you that providers **never really turn for the better** - if someone didn't have privacy / user respect as their priority right from the start, at best they might earn a passable grade. An easy way to bring yourself up to speed is to make browsing communities like Reddit's privacy boards or our group chat a regular occurence, or subscribing to news feeds such as GHacks or TorrentFreak. In any privacy community there will be different people who read various other sites, so they could tell you about stuff you'd never encounter on your own - so I guess that is the best way to stay informed.

Back to the front page