Some Fundamental Principles

This page is a complement to this one. If you've arrived here through another path, you should read it first.

Let's start with some definitions to ensure we're on the same page:

- **Privacy:** This refers to the right to control the information you share about yourself. When it comes to the internet, privacy often refers to the protection of personal information that you share online, whether voluntarily (for example, when creating an account on a website) or involuntarily (for example, when your IP address is recorded by a website you visit).
- **Anonymity:** Online anonymity means that your real identity is unknown. This can be achieved in various ways, such as using a pseudonym when posting comments online, masking your IP address to hide your real location, or using private browsing tools to prevent tracking of your online activities.
- **Security:** In internet terms, security refers to protection against online threats. This includes protecting your personal information from theft or exploitation, safeguarding your computer from malware and attacks, and ensuring that your online communications are secure and cannot be intercepted or decrypted by unauthorized third parties.

In short, these three concepts are related but distinct: privacy focuses on controlling your own information, anonymity focuses on concealing your identity, and security focuses on protection from threats.

It is crucial to remember these distinctions because a situation might be excellent in terms of security but very poor in terms of privacy, or vice versa. You may be forced to make choices favoring one of these notions at the expense of another. It's best to make these choices with full awareness.

Prioritize Open-Source Protocols and Software

While it's entirely possible for proprietary software to be secure and respectful of your privacy, it's essentially impossible to be certain without access to the code. As a result, open-source software has a structural advantage in this area, and **you should favor them whenever possible**.

However, be cautious, as this is **by no means a guarantee**, and simply using open-source software and protocols is not enough to secure your practices.

Identify Your Needs, the Challenges, and Know the Limits

When it comes to security and anonymity, there is no one-size-fits-all solution. Some compromises may be too burdensome for your daily use but will be indispensable if you're aiming for advanced anonymity.

To be effective, you will need to identify your situation and your needs and adopt practices specifically tailored to them.

Beyond a few best practices that apply to all situations, you'll need to have a relatively precise idea of what you're aiming for (for example, the challenges will be very different if you're seeking complete anonymity, private communication, or ensuring a specific identity), the technical means to achieve it, and their limitations.

Principle of Least Privilege

Think about your home and the keys you distribute to different people. You give your children a key to the front door, but probably not a key to your diary or personal safe. Everyone has only the access necessary for their role. This is the idea of the principle of least privilege. **Every user of a computer system should only have the minimum permissions necessary to perform their tasks**. For example, if you share your computer with other family members, you probably wouldn't give your children the same level of access as you have as the computer's administrator. This helps prevent potential issues, such as accidentally downloading malware.

This principle applies broadly: **do not give any unnecessary permissions to third parties**, especially if these third parties are private companies whose business revolves around collecting data about you.

Minimizing Exposed Data

If you're hosting a party and ask your guests to sign up in advance, you'll probably need their name and maybe their email address to send them party details. But would you ask for their social security number or date of birth? Certainly not, because **such information is unnecessary for organizing the party and, if lost or stolen, could cause a lot of problems** for your guests. This is the concept of data minimization: **only collect, store, and use the data absolutely necessary to complete the task at hand**. This reduces the risk of data theft because fewer sensitive data are stored, and there's less data that could be exploited.

This fundamental principle mainly applies to service operators, who handle large amounts of data. But you should also apply it individually. Do not divulge any data or information about yourself that is not strictly necessary to achieve your objectives (not those of the service provider).

Systematize and Formalize Practices

The best security practices won't protect you if you don't apply them. This is obvious, but it doesn't stop even the most knowledgeable people from letting their guard down, missing something, and making a mistake that could undo all their usual efforts.

Once you've identified your needs, **it is essential to formalize and systematize the practices that meet them**. Some of these will be easy and can be automated, but in many cases, you'll have manual interventions to make (for example, to encrypt a message or choose between TOR and a VPN). Like all

habits, it’s difficult at first, but it becomes second nature quickly.

Security, Web, OpenSource