Privacy regarding the internet is centralised around withholding information from third parties [1]. These can be companies, organisations or other people.

The term privacy originates from French, privauté meaning free from intrusion.

The issue of privacy is perhaps more relevant than ever. In a digital age where everyone is interconnected, learning something, stalking someone or researching something has never been easier.

---

Privacy is simply a state of not being observed. It can come in many forms such as closing the door when you go to the toilet, or not telling people you met at your cousin's wedding that your best friend is a pebble. Privacy becomes important when dealing with large amounts of information in a public context. Like water, information will flow and reach everywhere it can go, once there, it can cause damage. While water damage can be repaired, informational damage cannot as the internet prohibits things from truly disappearing. The damage will most likely be cybercrime related such as identity theft or intellectual property theft.

---

Internet users have huge amounts of data that is considered "private" without them being explicitly aware of its presence. This makes it easy to find patterns and compile hints about any person or company. Not only does this allow for identity theft and numerous other cybercrimes but it also puts other connections or contacts at risk.

---

As a programmer, I spend a lot of time interacting with computers and other computer users, this not only leaves me plenty of time to open vulnerabilities into my own world, but everything I have worked on and every idea I've ever tested. Not only am I closely connected with computational systems, I take interest in designing them and their communications networks. A major part in systems design is knowing how to properly secure them. Also interesting but not my main interest is the study of their vulnerabilities. Careers exist around exploiting weaknesses and are some of the most high-paying professions in the computing industry. It is this as well as many other reasons that personal privacy on the internet must remain one of my top priorities.

---

Information is easily secured, just jumble it up so that no one can read it - easy. The problem with this is that it must be reversible in order to understand what is meant. Making it reversible however, will allow anyone to decipher it. Instead, an entire field of mathematics exists that is devoted to developing algorithms that can reversibly scramble information so that it is only undoable by those who know how it was originally scrambled. While it is easy to protect information, it is not so easy to conceal personal data such as your shopping history or your contact list from collectors as they will find any way to continue collecting.

Using airline companies as an example, they store cookies (small pieces of information) on your computer to calculate your flight path, flight details, destination, departure times and everything related. They then bias the prices in order to make the most money out of you. In addition to this, advertising companies such as Google, Facebook and YouTube will show advertisement related to your search and engagement histories (information that you react to such as posters, images, ads or articles). This is designed to give you an overview over the range of prices versus quality. This is then used to lure you into buying commercial flights that aren't that great but still charge top dollar.

While targeted advertising is great for understanding a product range, it is exploited by large companies because of how much information is behind them. Google even goes to the lengths of recording what you're saying when you have its Chrome browser installed on your system to further fuel its ad campaign. This means that Google not only knows everything you're interested in, but Google also knows who your friends are, where you live, what you look like and what you sound like, *and* they *never* forget. A great way to prevent this is to use *Open Source* software meaning its source code is available for anyone to inspect and play around with. This provides transparency in the software and hence a layer of trust.

Generally speaking, major companies' largest projects won't be open source but alternatives will almost certainly exist that are. For example, Google's Chrome browser is proprietary software but alternatives such as Mozilla Firefox are open source. Another alternative to protect yourself is to use sensor scrambling software. These act like middleware to your computers sensors such as the camera, microphone and GPS by turning the output data from the sensors into gibberish and ensure it cannot be accessed unless the user has granted permission. Generally, protecting yourself is as easy as not using the biggest company available. The Google search engine has countless alternatives whose mission it is to provide privacy to you. One such search engine is DuckDuckGo - my personal choice.

---

If you've ever used the internet, then this is you. Every piece of information about you is exploitable meaning the more that's known about you, the more vulnerable you are.

---

[1] <https://www.lexico.com/en/definition/privacy> (Oxford):

Privacy: a state in which one is not observed or disturbed by other people.

[2] <https://en.wikipedia.org/wiki/Cryptography> (Wikipedia):

Cryptography / Cryptology is the practice and study of techniques for [secure communication](https://en.wikipedia.org/wiki/Secure_communication) in the presence of third parties called [adversaries](https://en.wikipedia.org/wiki/Adversary_(cryptography))

---

The current era has been coined the Information Age because of the shocking amounts of data that are being passed around, collected or generated. With volumes of this scale, not all of it can be properly managed. This is where privacy issues become relevant. As data is being collected from every internet user around the clock, a picture or profile can be drawn to represent that person. Generally, any data that can be found will be recorded. Software such as the Google Search Engine or YouTube will customise content specifically to match this user's interests, allowing these platforms to feed information that show exactly what the user is looking for. The issue with this is that information can be customised and show biased and less reliable information, hence an incomplete overview of the subject. In addition to this, personal details can be used to recognise patterns and fake profiles can be established in this image, resulting in identity theft potential and other forms of cybercrimes. I deal with information systems frequently leaving me vulnerable to such data mines. Since I deal with such large amounts of data, I need to know how to protect myself against it. I learned this first-hand when I created a Google account. Without me having to specify, Google immediately knew my age, location and gender. Being stunned, I entered bogus information. A few weeks later, I came across my Account preferences and saw that google had corrected the bogus information I had entered. I chose to use a website to present this issue as it would allow me to embed more realistic examples to further demonstrate this issue's scope. I also had it ready for me to quite literally, Copy and Paste the sections of my response into it. The website's template I used was originally designed to be an informational website targeted at anyone researching companies, products or people. The final website will be targeted at reckless internet users to attempt to persuade behavioural change. Throughout the website, I used informal language to make it feel more like a conversation and make it more engaging. I used similes and metaphors to make the topic more understandable to someone who may not be familiar with privacy issues. There is also persuasive language scattered throughout the website to convince readers to change their behaviours.