**Risks:**

*What risks can you identify for your project? There will always be some generic risks (such as computers breaking down the night before a deadline, health and family issues, and institutional changes). Do not include generic risks such as these. The idea is to be as specific as you can to your project. For example, if your topic is to develop a game, there may be a risk that the software you choose to work with may be very difficult to learn, poorly documented, or not turn out to have the features that it claims it has. These properties are often only discovered once you have started working with the software, and so unless you have had lots of experience with the particular tool, there is always a risk that it may not work as well as you believe it should, no matter how much prior research you do. Similar comments apply to hardware.*

There are various risks to the project ranging from software related issues such as software used to program this project, to privacy concerns such as what information will be retained if any to security issues such as safeguarding against various security breaches where data can be stolen, especially personal and confidential data.

Software risks are minimal though sufficient enough to pose delays in terms of training or incompatibilities with the project. In order to construct this project it will require someone who is proficient with programming languages (Such as JavaScript, C++, etc) and Markup languages (HTML), will require someone in Systems Administration & Networking to setup servers and networking services for this project so that users and the software are able to communicate between each other & the servers they are hosted on. As this project will likely be developed on mobile devices such as iOS & Android, people who are capable of programming and implementing the project on these devices will be needed as well. If people are not quite fully equipped with certain tasks to use certain programming software then time aside will be needed for training as well as looking into programming languages and programs that are cross-platform compatible if a wider market is to be reached.

Privacy is a major concern and risk of this project tying into the security risks of this project as well. Given the fact that this project tracks search history, live search results and in extereme cases of physical, sexual abuse or child explotation (be it from searched results on the internet or chat from a child to a live bot), what is being stored and what isn’t could be a privacy concern especially if personal information were to be stored (In this project itis unlikely that accounts are to be created with required information). Given the sensitive subject at hand, the privacy matter may be an issue with getting the software distributed in certain regions such as the European Union who have strict laws on tracking and using data, stored or not, as well as the ethical matters of having software tracking such sort of things despite the targeted audience from a legal perspective needing their parents permission and guidance for most things anyway, not just limited to the internet.

Security is a big risk for this project and considering the sensitive data that could be stolen can have real world risks to a person’s mental health. Depending on the implementation of this project in regards to how users sign up and sign into our service, if there is a data breach on Open Mind’s servers then potentially any sign in information such as their real name, e-mail address, street address or any other personal information could be leaked and stolen if proper safe guards aren’t implemented, especially if the user’s computer is infected with malware such as a keylogger that records a user's keystrokes to steal passwords and other confidential information. Speaking of data breach, if Open Minds decide to branch out the software to mobile platforms such as IOS & Android to be distributed through Apple’s Apple Store or Google’s Google Play, it would have to rely on Apple & Google to ensure their distribution stores as mentioned above are secure and not disturbing malware that can steal data, which is highly unlikely as seen [here](https://www.forbes.com/sites/kateoflahertyuk/2019/10/24/new-google-android-malware-warning-issued-to-8-million-play-store-users/#2a3608b51235) with Google and [here](https://www.popularmechanics.com/technology/apps/a29575329/iphone-apps-malware/) with Apple.

Adding on to distribution methods, since this project is primarily aimed at being added via browser extension (such as AdBlock Plus), if it is hosted on Firefox/Google Chrome’s Web Store then depending on how the extension is created, any new exploits targeting certain website protocols or codes will be need to be patched and monitored to avoid data breaches. If our project is being hosted on a  website itself (such as our company website), the website will need to be safeguarded from any malicious breaches (Cloudfare is an example of what this website could be protected as they offer services to protect from DDoS attacks or provide SSL/TLS encryption).