Security, Privacy and Legal Issues

Robert Iarinka

April 2024

1 Introduction

In this document I will be going through the different Security, Privacy and Legal Issues i was faced with and how through correct implementation i was able to make sure user data is protected.

2 Security Issues

When designing an Social networking website there are a lot of different factors that need to be addressed and taken into consideration. These factors range from ensuring we are protecting our users from potential attacks on their private data, such as DDoS attacks, phishing.

3 Measures Taken

One pivotal security measure implemented in our system is password hashing. Hashing transforms the original password into a unique set of characters via a hash function. Unlike encryption, which is designed to be reversible with a key, hashing is a one-way process. This means if an unauthorized party accesses the database, they cannot reverse-engineer the hashed passwords to discover the original plain text versions. I also used bcrypt to further ensure the data is secured. I also tired to use server sided encryption, that meant that if someone had managed to enter the database they wouldn't be able to access the passwords as they are encrypted.

4 What could be improved

In the current implementation of my Social Networking Website the messages between users are not end to end encrypted. This can be seen as a

security vulnerability and potential Privacy and legal issue.

5 What needs to be Implemented

Implementing a signal protocol which is one of the most efficient solutions for strong End to End encryption for the messages.

Self-Destructing messages might provide to a good solution, which would delete older conversations at the agreement of the user.

6 Privacy Issues

When designing the Social Networking website I was faced with a lot of potential privacy. The main challenge at hand was to collect only the most essential information required for optimal functionality and user experience, thereby minimizing the risks associated with data storage and management. There are a lot of privacy issues that needed to be addressed such as taking user information and such as passwords, emails, and phone numbers.

7 Measures taken

The main measure taken are that when a user registers an account with us not a lot of information is asked of them, and currently is not used by third party tracking, and there is no data aggregation.

8 What could be improved

Currently there isn't much that can be improved as there isn't much implemented that leads increased levels of privacy. The ways we use cookies can be improved so that we make the user aware of these and tell them exactly what type of data we will store and if they agree to them or not.

9 What needs to be Implemented

Features such as User-Controlled Data Deletion with the purpose of allowing users to easily delete their accounts and associated data permanently from the platform. Two-Factor Authentication (2FA). Introduce 2FA to add an extra layer of security for user accounts, protecting against unauthorized

access. Privacy Settings Interface. Develop an intuitive interface for users to easily adjust their privacy settings, including data sharing and visibility.

10 Legal Issues

When operating a social networking website, there are several legal issues to consider that relate to user privacy, data protection, intellectual property, and compliance with specific laws and regulations. Addressing these legal aspects is crucial to avoid potential lawsuits, fines, and reputations damage. Compliance with data protection laws such as the General Data Protection Regulation (GDPR) in the EU, California Consumer Privacy Act (CCPA), and other national and international regulations is critical. These laws dictate how personal data should be collected, processed, stored, and shared.

11 Measures Taken

The main measure I took was encryption of passwords and hashing of passwords to ensure extra security on the sensitive information and made sure that brute forcing passwords is also harder as the specific phone number is needed.

12 What can be improved

Introduce more granular privacy controls that allow users to customize exactly who can see their posts, personal information, and activity. Provide clear explanations on the implications of each setting as well as Upgrade encryption methods for data in transit and at rest, incorporating newer algorithms that ensure greater security. Implement end-to-end encryption for all personal and sensitive communications.

13 What needs to be implemented

Integrate 2FA for all accounts to provide an additional layer of security beyond just the password, significantly reducing the risk of unauthorized access. Implement End to End Encryption for all private communications between users to ensure that messages are readable only by the sender and

recipient, not even by the platform itself, so that way we ensure full privacy for the Users.

14 Threats To the Social Networking website

One of the main threats to my social networking website is a phishing attack, as this can cause a massive leaked of private information of users, as out website handles users personal email accounts, there is always a risk of these getting attacked, there are also chances of a user getting tricked into giving out their personal details to the wrong people. This threat however can be solved using 2FA and secure communication channels, and ensuring that all of our users are safe and protected from other malicious people asking for private information when discussing in the website.

Another threat is social engineering as this is a manipulative technique used to exploit humans and gain access to private information, this can also happen while users are conversing, a user can be tricked and manipulated into giving information away as well as staff being manipulated and giving access to private information. This threat can be dealt with training staff, and ensuring that all users that register to our website need to have 2FA and be verified with an ID.

Another treat is Key loggers, this treats is very dangerous as it can easily by-pass our encryption and allow access to sensitive and private data of a user. Key loggers are a type of monitoring software designed to record keystrokes made by a user. This is a form of spyware that can let a malicious person get access to all the information recently typed by their user, this can be emails, password, phone numbers etc. However this threat can be mitigated by ensuring all data transmitted to and from your site is encrypted with HTTPS to protect it in transit and offering the option to use a virtual keyboard.

15 Conclusion

In conclusion those are the Security, Privacy and Legal issues i was faced with and through my social networking website implementation I tried to ensure the requirements for all have been meet.