MYLogin: A Local and Secure Utilities Solution

Mateo Alado, Pavlo Sernetskyi, Alexia Herbert, Stephanie Phan

Department of Computer Science, California State University, East Bay

CS 230: Computing and Social Responsibility

Dr. Lynne Grewe

September 23, 2024

Ethical Business Plan:

A. MYLogins - A Local and Secure Utilities Solution
Company Name

B. Long-Term Vision Statement

1. **Goals**
   The goals of the MYLogins platform are to protect and organize user login data, through local secure storage. The platform aims to streamline data security with a goal of full user privacy, while maintaining compliance with federal data protection laws. MYLogins will evolve to achieve full platform independence, portability, and cross-platform compatibility, expanding to include commercial and enterprise options.
2. **Idea Origination**: where did your idea come from (a class, a job, a need)? (Mateo)
3. **Purpose/Values/Mission:** what is the purpose, values, and mission? (Pavlo)

The purpose of MYLogin is to provide a secure open source platform so that the diverse groups of users can safely store and use their login credentials. It also ensures full control over their data since it does not rely on any third party cloud providers and is securely stored offline. MyLogin was designed to meet the needs of individual users and enterprises as well. In addition, MYLogin values privacy, transparency, and community-driven open source development. Finally the mission of the MYLogin is to empower development of the ecosystem that promotes protection of sensitive information using the latest encryption algorithms and timely bug fixes. One of the key concepts is promotion of collaboration and engaging diverse groups of developers to contribute to open source.

4. **Key Questions:** List 2 or 3 key questions that will guide the startup's choices. These should be essential questions that serve as touchstones to direct your company's efforts. For instance, how can the startup have an impact? What engages our passions? (Stephanie)
    a. How do we make the start up more accessible for stakeholders?
    b. How can MyLogins protect the privacy of their users?

C.
OKR 1: Platform Independence, Portability - Alexia, Stephanie.
Alexia:

C.1:

MYLogins LLC aims to achieve full platform independence as its objective. A key result of this objective will be launching MYLogins on iOS and Android platforms by the end of Q2 2025, ensuring functionality and compatibility with mobile devices. Deployment of the MYLogins application for mobile devices will allow the startup to widen and diversify its user base, reaching individuals who primarily use their phones as well as businesses looking to implement multi-factor authentication via authenticator software.

C.2:

A way to measure the success of the MYLogins iOS and Android deployments is by looking at the analytics from the Apple and Google store. The startup will review the analytics of how many times the application has been downloaded and can gauge the success of the application considering this as a factor. We will set a goal of 10,000 downloads by the end of the first month and see how well it holds up to this metric. We can also look at internal data in order to see the trend in active daily users and set up a goal for a retention rate, revisiting these statistics after the first month. Lastly, we can reference user satisfaction as a metric. More specifically, gathering data from application reviews in the apple and google play stores and maintaining a 4 star rating would be a metric for success. Another route to take is to send out customer satisfaction surveys and have a goal of 80% average reported satisfaction.

C.3:

Ethical impacts that we can face at MYLogins includes deploying applications that are not inclusive to our user base. This would hurt our user numbers, creating obstacles for those who feel excluded and thereby discouraging them from using the application. Another ethical impact is the use of user data. Our case study on the court case of ACLU v Clearview AI explored the consequences of misusing user data. Clearview AI was held liable for not notifying users and getting consent for scraping user data to train their artificial intelligence [1]. If we do not consider how our internal user data will be handled, and develop policies and procedures to manage it, we may end up violating user privacy laws and put our company at risk for legal

litigation. Being a startup whose product markets user data management and data protection, we need to have airtight policies that are compliant with data laws.

Stakeholders	Financial Risk	Privacy Risk	Conflicting Interest Risk
MYLogins LLC	High	Mid	Low
Customers	Low	High	Mid
Online Application Stores	Low	Low	Mid
US Government	Low	Mid	High

In our risk table, we have four main stakeholders: MYLogins LLC, our customers, online application stores, and the US Government. The financial risk for MYLoginsLLC is high given startup costs for the development and maintenance of security systems in addition to the potential for huge financial penalties if compliance is not met. The customers, online application stores, and US Government all have low financial risk. Firstly, the application is free, so overall user cost should be very low. Application stores like Apple and the Google Play stores have minimal financial risk, but may face reputational risks if the app has privacy issues. The government is not directly affected by MYLogins success, but enforcement of data compliance procedures can be a factor. Privacy risk for both MYLogins and the government are mid level. MYLogins must handle sensitive user data, and in the event of a breach may face reputational harm. Government privacy risk is mid, given that the role of the government in regards to data protection is to ensure the privacy of citizens data. Customer privacy risk is high due to individual customer login credentials and sensitive information being stored in MYLogins servers. If data gets breached, this can put customers at risk for identity theft and fraud. Application stores have low privacy risk, since they will not be handling sensitive MYLogins data directly. Conflicting interest for MYLogins LLC is low, since the company objective is to safely store and secure user data. Conflicting interest may include the conflict between maximization of profits and investing in more security measures. Conflicting interest for customers and online application stores are both mid level, as customers are looking for data storage and privacy while company use of data may be for analytics and improving services. This is a potential conflict of interest. Online application stores have a mid level conflict of interest between showing popular revenue generating applications and ensuring that security standards are being met on the applications they host in the store. The government has a high risk for conflicting interest, as it may have interests in data access for federal purposes, which may conflict with MYLogins individual privacy and responsibility of data protection for its customers.

C.4:

An ethical safeguard to consider with the development and launch of the MYLogins iOS and Android applications is inclusive beta testing. In order to optimize the application to be its most efficient, we need to consider users of all demographics. This allows us to receive feedback from all backgrounds and minimizes a biased view. We can consult diversity and inclusion professionals in order to receive guidance on the best way to make our platform inclusive to all users. Additionally data privacy is an ethical concern when handling user data. We need to ensure that MYLogins is compliant with the laws around data privacy and has security implementations to protect this data. Data transparency is something we reviewed for our case study assignment and it applies here as well. MYLogins LLC will need to inform the user if their data will be gathered and get user consent. We aim to minimize the utilization of this data, and will not sell to third parties. Additionally, we can consult lawyers who specialize in this sector and implement protective solutions based upon their guidance.

OKR2: Privacy - Mateo.

Company Summary:

At MYLogins, we strive to deliver a product that aims to reliably automate the task of login credential storage through our storage and retrieval platform. Aimed primarily at individual consumers and small enterprise businesses, the MYLogins application provides an innovative local/server hybrid storage model, allowing for users to write login information and associated credentials to specialized local storage that is stored safely in the user's filesystem, and offers numerous option for editing and version control. Subsequently, login information and other user data is then encrypted and sent to a secure server location for backup as specified by the user, thereby ensuring a high degree of security and reliability for later access and use.

Objective and Key Result (OKR):

A major goal of the platform is to ensure the privacy and security of the user information via maintaining the integrity of the platform's encryption and local storage. In regards to the various stakeholders, MYLogins is designed to protect our individual consumer base and enterprise business clients from malicious third parties. Keeping in mind the differences in consumer and enterprise objectives and data storage projections, MYLogins is primarily and largely focused on the consumer user base given our commitment to maintain privacy and is therefore given the most attention in regards to application design, however there is still strides taken to accommodate businesses' privacy as we feel that data integrity should be available to all entities.

Ethical Impacts and Issues:

Regarding Ethical Issues with MYLogins, the main concerns with the platform and application largely revolve around the potential breach of information and data in regards to enterprises. Because the platform largely relies on local device storage of data as opposed to migration to a larger centralized database, the primary concern lies in the fact that some information may be vulnerable if the load is significantly bigger, thereby making the application impractical to use for some business entities. Additionally, we must also address concerns involving licensing, as though we are a company that uses open-source software, we must also reconcile this fact with the need to generate profit through selling the product, therefore posing a possible issue in the form of pricing.

Ethical Safeguards:

Keeping in mind the various ethical and concerns and issues previously mentioned, MYLogins must put in place a safeguard in regards to reinforcing our platform to ensure total privacy for larger business enterprise clients, and must therefore update our application utility in order to accommodate larger loads of data by integrating secure databases that both encrypt datasets and ensure various network protections. In regards to the issue of pricing

OKR3: Open Source Software - Pavlo

C.1:OKRs

The main objective of MYLogin is that it operates as open source and available for users to distribute, modify or view thus promoting transparency and security. It also encourages other developers to contribute to improving documentation, collaboration on the new features and finding bugs.One of the driving forces and motivation for creating open source software is the spirit of collaboration: “At the heart of open source is the spirit of collaboration and community. Developers from around the world come together to contribute their expertise, share ideas, and collectively solve complex problems. Through online forums, mailing lists, and collaborative platforms like GitHub, individuals can collaborate on projects in real-time, driving innovation and pushing the boundaries of what's possible” [1]. Having a diverse team of developers is one of the most important things to promote development while setting the right goals or key results is an essential thing that will lead business to success. One of the key results for the next 6 months would be to attract 50 new active contributors who will actively contribute to the open source software.

C.2: Metrics

To measure success metrics we would need to know many new contributors we get each quarter. This can be done by monitoring GitHub activity while keeping track of the number of the pull requests created by developers, which directly correlates to the process of software development.

C.3:Ethical Impact(s)/Issue(s)

One of the big ethical issues in open source software is related to bug fixings. It’s important to fix bugs before they get publicly exposed. Imagine some bad actors gain access to exposed software and get access to all of the sensitive data stored. Despite MYLogin offering a secure offline repository for managing login credentials, it still poses vulnerability risk: “In open-source projects, all the code is available to anybody, so people within the community can pool resources and identify flaws in the code, repairing the issue before announcing the

vulnerability. However, since all vulnerabilities become public information on the National Vulnerability Database (NVD), attackers can use this same information to target an organization that still didn't apply the patch" [2]. The patching and proper, timely bug fixing ensures security before vulnerabilities are exposed thus reducing risk of malicious exploitation.

C.4: Ethical Safeguards

To mitigate risks of exposing sensitive data, open source developers should focus on timing of bug fixes which is a critical part of open source software development. In addition, developers can consider enhancing software with a strong encryption algorithm AES-256 which would encrypt the repository that contains all sensitive credentials. MYLogin stores information locally so these files will benefit from the following improvement: "Encryption is an excellent option for mitigating file sharing security risks. It works by taking plain text or data and using a key to convert it into a code called a cipher. Cipher code is an unreadable and effectively indecipherable text that neither humans nor computers can understand" [3]. To incorporate this ethical safeguard the process would involve ethical experts who specialize in data privacy and software security professionals such as white hat hackers. They can be hired internally or through an open source community. Incorporating encryption would involve several phases such as gathering business requirements, planning, development, testing and deployment. The effectiveness of this solution can be measured with penetration testing when some other professionals would get permission to hack the database and gain access to sensitive data thus exposing any existing bugs or vulnerabilities in the system. To get tangible metrics we can evaluate the reliability of an existing system by the number of times it can be penetrated thus providing feedback on the robustness of the existing system.