CS230 Section 1

Group 10

4/25/2025

Paul Cooper
Glenn Cristobal
Phat Khuu
Benjamin Samok

Entrepreneurism & Ethics

1: Ethical Business Plan

1.A. Company Name

Beulai (pronounced Bueller)

1.B. Long-Term Vision Statement

1.B.1 Goals:

When users sign up to use a website or other online service, they must agree to the terms as stipulated by the company providing the service. These forms have become intentionally more complicated over time, using legalese that at times is hard for most people to understand. Knowing most end-users won't read through longer terms of service agreements, most companies have increased the length of these documents and made them unnecessarily long to expand their control over of customer data while limiting their own liability [1]. Beulai's goal is to help end-users take back some control over these agreements by having AI summarize the end user license agreements into a short, easy to understand document. Since it will run as an extension in a browser, it will also notify end users when the terms of service have changed for a particular website since the last time the user visited that site.

1.B.2 Idea Origination:

The idea came about after many years of listening to technology focused podcasts. It became clear while listening to the news stories that when the terms of service changed, they always favored the company. Stories such as Amazon including a zombie apocalypse clause into their video game development software [2] or Facebook forcing WhatsApp users to share their data with Facebook despite previously having pledged never to do so [3]. This led to millions of their users switching to Signal and Telegram rather than
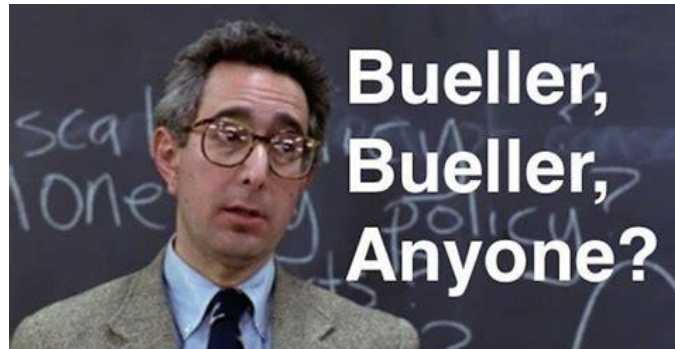
accepting the new terms. One game seller in England even jokingly added terms that granted them the "immortal soul" of 7,500 new customers who accepted their terms as an April Fool's joke (they have since nullified this clause) [4].

With most users never reading the terms in the end user license agreements and many companies knowingly taking advantage of a system that clearly is not fair or balanced, there is a clear need to monitor the terms of service websites are currently pushing on their customers. Some of this is being done on a small scale. The EFF (Electronic Frontier Foundation) for example does host an api and GitHub repository that tracks the changes made to the terms of services agreements for most popular websites. Giving end-users the ability to read a summary of the terms before agreeing to them and also providing near real time updates when the terms of service change should provide much needed transparency to our customers where there is currently a glaring lack of information.

1.B.3 Purpose/Values/Mission:

Beulai is a privacy centric company whose mission is to expand our users' understanding of the privacy and rights they are giving up every time they agree to the terms presented to them when they accept an end-user license agreement. We strive to provide an accurate summary of the terms and conditions presented to them by other websites so that they can make an educated decision when they accept the terms of an agreement without having to read the entire contents of that agreement. To that end, we must provide our services with the promise to limit any personal data we collect to a minimum, delete any personal data as soon as it is no longer needed, and promise never to share this information with any other parties unless legally required to do so (such as through a warrant or court order). As more customers use our service, we hope to grow an educated user base that will spread our privacy first message to their friends and family and eventually reach a tipping point where companies must provide fair and balanced terms to their customers either due to user churn or as required by law implemented by state or federal legislatures.

1.B.4 Key Questions:

As Beulai establishes itself online and starts to grow we must continue to ask ourselves the following questions to make sure we stay true to our original mission and goals as we pivot in response to our customers' needs. How do we provide the service in such a way that we don't need personally identifiable data from our users? Once our initial product is up and running, how do we expand our offerings while still enforcing the requirement that no personal data is required from our user base? Finally, as we grow, we may need to update our own terms of service and we need to ask ourselves, from an end users perspective, whether our own terms match our principles and offer fair and balanced approach that maintains our customers rights and privacy.

1.C. Strategy with Ethical Impacts AND Ethical Safeguards:

1.C.0: Company Summary

When most users sign up for an online product or service, they are generally presented with an End-user License Agreement (EULA) or terms of service agreement. These EULAs have a reputation for being long and often filled with legal jargon, making the process of reading and understanding the agreement rather cumbersome, to the extent that most users just agree to the EULA without reading it. According to a Deloitte Survey in 2017, 91% of participants agree to the terms of service without ever reading them [5].

Beulai's (pronounced Bueller) goal is not to get end-users to read the terms of service, but rather to provide an AI generated summary of the EULA which is quick and easy to read and understand. There will be a website where you can look up any EULA with the Beulai provided summary at any time, but there will also be an accompanying browser extension available. When a user visits a website for the first time after having installed the extension, Beulai will provide the summary of the EULA. We will generate and store these summaries on our servers to reduce the overall amount of processing required. We will periodically rescan every website EULA and ToS pages to check for changes to the agreements. This will allow us to compare different versions of the original agreements and our summaries overtime. When these agreements change, we will be able to provide our users with an updated summary of the agreements if the EULA has changed since the last time the end-user visited the site.

1.C.1.1 OKR 1 Objective and Key Result

There are millions of websites that customers browse every day across the planet. For Beulai to provide a good customer experience, we want to be able to provide a summarized EULA for every site our customers visit. Not all sites provide terms of service, but for those that do, it is Beulai's goal to provide a short summary of the terms of service to all of its customers. To that end, we need to start with the most popular websites having already been scanned and grow the list from there.

The initial goal is to be able to provide a summarized EULA for 95% of websites that customers visit. We should be able to generate a pretty thorough list of the websites visited most often before going live with our initial public release. Inevitably though, we will miss some lesser used sites, and new websites are created daily. To add sites we don't initially include, we will take note of unlisted sites as our customers visit them. The browser extension will need to check in with Beulai to determine whether the terms of service have changed since the customers' last visit. If a customer visits a site that is unknown to Beulai, this can be logged, and action can be taken to make sure we summarize the terms for that website during our next batch of EULA scan updates.

For Beulai to be successful, it must keep its customers up to date on the changes made to the terms of service other websites publish. Because Beulai's customers want to know more about the terms they are agreeing to when signing up for services, we recognize that our customers are, in general, more concerned about privacy than most other users and in turn we must be transparent with our own End-user agreement and make it clear that we will store as little information as possible to provide the services we offer and that our customer's data is not, cannot be, and will never be for sale. In the long run, as Beulai grows, and customers become more familiar with the terms they are agreeing to, the hope is that they can in turn step up the pressure on other service providers to improve their own terms of service and start to generate business models that don't require the selling of user data to make money or at the very least make sure their customers are willing participating in the sale of their personal data.

1.C.1.2 OKR 1 Metric(s) with Experiment(s)

Any given interaction with a customer is considered a success if we can provide a summary of the EULA for any given website our customers visit (assuming they have terms of services listed). For customers using the browser extension, for every website they visit, we need to perform a quick look up to determine if we have the EULA summary on file. Assuming we have the summary on hand, we log it as a success (along with the domain and the timestamp). If the summary is not available, we log it as a failed attempt (along with the domain and timestamp). When a failure is logged, it will trigger a search of that domain for the terms of service to be analyzed during the next batch run. Since the most popular websites will occupy most of the EULA summary requests, we expect to obtain a high success rate in a relatively short period of time as we have a built-in mechanism to search for any missing End-user license agreements. Allowing for subsequent requests to for that summary to be successful. The goal is to reach 95% success rate within the first quarter and continue to increase the success rate as we progress.

1.C.1.3 OKR 1 Ethical Impact(s)/Issues(s)

Our goal is to educate End-users on some of the shadier details that are included in typical End-user license agreements. This includes the logging and storing of End-user personal data. Most users today are aware their data is being sold, but without reading the EULA's they are unaware specifically of what data is available and to whom it can be shared with. Along with sharing and selling this information with other companies, the supreme court has affirmed that the Fourth Amendment allows the government to request and obtain information revealed to a third party. When an individual voluntarily shares information with a third party, they lose their reasonable expectation of privacy to that information [6].

Beulai is primarily a browser extension and will need to have a public facing API in addition to a website. As envisioned, Beulai will not need to store any personally identifiable information, but basic security measures such as a WAF and firewall will require user IP addresses to be logged. While the logging required to measure the summary success rate would not include the IP addresses, the WAF may need to log the users' requests which, barring any malfeasance from the user, should only include an authentication token, a domain, and a timestamp of the last time the customer visited that domain. Since we intentionally don't store personally

identifiable information, we cannot share or sell our users data to other companies or law enforcement, maintaining our customers privacy as much as we possibly can.

Stakeholder Risks

Stakeholder	Financial	Privacy	Conflicting Interest	Violation of Rights
Customer	Low	Med	Low	Low
Beulai	High	Low	Med	Low
Regulatory Bodies	Low	Low	Low	Low
Tech Companies	Low	Low	Low	Low

Customer Risks:

With the WAF logging both IP addresses and user requests, it could match a user, by IP address, to their browsing history. This would not usually be a one-to-one match as most IP addresses have more than one user, and there could be multiple users and devices using Beulai, so there would most likely be some obfuscation. That being said, it is not without some risk to our End-users.

Users are relatively safe from hackers, as if they were to break in, they would find little information on Beulai's servers tying back to a user. The hackers, once past the security devices, would need to then break into those same devices to get any user data, which is unlikely. Even if they do successfully break into the WAF and grab the logs, to recreate the browsing history would take some effort and at best they might be able to determine what sights a specific IP address visits, which might include financial sights, email, social media and other sensitive domains, but would in no way contain any user credentials or personally identifiable information.

It is possible that law enforcement could come to us with a court order or a warrant requesting specific data. At best, this could provide some private browsing habits for specific IP addresses. The chances that law enforcement would come to us to get this information is slim since they would generally target user's ISP's first, since they generally track their customers' browsing habits already, including DNS data which would provide better data than we could provide. In general, our customers risk little using our services, with privacy

being the biggest concern because of the browsing history that could be deduced from security logs, all other risks being low.

Beulai Risks:

As a new company, in a new space, Beulai does have a big financial risk. Any money used to develop and grow Beulai is at stake. In relatively short order, we need to minimize expenses to help bring in more revenue than we spend. Since scanning for EULA's and summarizing them is a relatively fixed cost, the faster we can grow our customer base, the quicker we can become cash positive. To that end, providing customers with the best possible experience should help grow our customer base. Providing a summary of the terms of services for 95% or more of the sites our customers visit should go a long way to driving more traffic to our service.

Regulatory Risks:

We are looking to store very little, if any personally identifiable information. Our services are looking to encourage a more private and secure internet. Even if our site were insecure, and we suffered a data breach, the data taken would be of little use to any potential hackers as EULA's summaries of websites probably are worth little to the outside world. They could steal Beulai's intellectual property, but customer wise, they would get little more than IP addresses with no names attached. From a regulatory perspective, we pose little risk to the public in general and are in fact working on their behalf to make the internet a safer place for all.

Tech Companies:

Other companies may object to our use of their EULA's for our services strictly because we may call out a term within their agreements, they don't want their customers to know about. While they may not like it, the point of these agreements is to inform customers of these terms. Arguing that we hurt them by exposing practices they already publicly admit to would hardly ingratiate them with their own customers. Scraping certain pages of a website is generally an accepted practice if it is done within reason. Search Engines, AI companies, and many other companies routinely scrape entire websites, if not the entire web. Most websites

have a robots.txt file to define what a bot can and cannot do while visiting a website. We are scraping for information that is publicly available and does not include any intellectual property when we scan a EULA/ToS page. We are well within our rights to gather this information and if challenged should be able to defend ourselves. We could also seek to get the backing of other organizations which advocate for more privacy online, especially someone like the EFF, which does have a limited service that monitors EULA's for the larger websites. Overall, the risk from other tech companies is low.

Since our users are anonymous to us, and we only log security and metric data, privacy risks are low, as are rights violations as we would only provide data to law enforcement through a court order or if warrant is attached to the request. There is a small risk of a conflict of interest as security personnel with access to our WAF could match user IP addresses to their browsing history. Other employees might have access to domains that our customers are browsing but would not be able to tie them back to a customer.

1.C.1.4 OKR 1 Ethical Safeguards

For the items listed above with elevated risk, we have already addressed the safeguards in place to reduce the risk. A quick summary follows. As part of building a new company, financial risk is inevitable. The financial risks associated with this venture are known up front to those involved. OKR's are being used to gather metrics and measure our success at reaching different goals. With these in place the financial risks should decrease by promoting customer loyalty and growth.

By designing Beulai in such a way that allows customers to read summaries of a websites EULA by only sharing the domain name with us, we eliminate most privacy concerns as we never have any personally identifiable information in our possession at any step of the way. The only information that can link back to a user would be an IP address stored in our security appliances. While access to this information is limited to a few users, there is still some risk of abuse. To minimize this risk a centralized logging system would be employed so that any access to these systems would also be logged. Role based access would also be employed to enforce only users that need access to these systems have access, this would also include the logging server. To enforce our internal controls, we would employ a third-party auditor to periodically (at least annually)

review our policies and procedures and verify that they have been implemented correctly and to suggest changes if they find any processes to be lacking when it comes to security or privacy concerns.

With these measures in place, we should be reasonably sure we can protect our customers and our own data from third parties, including the government. With our emphasis on never storing personal information, and storing as little data as possible, the risks of exposing our customers' data are minimized. This will allow us to focus more on our goal of educating our users to the rights they are giving up when they accept the terms without reading them. We hope to encourage our users to push back on other companies and start fighting back to protect their privacy. "Arguing that you don't care about privacy because you have nothing to hide is like arguing that you don't care about free speech because you have nothing to say [7]."

1.C.2.1 OKR 2 Objective and Key Result

Across the Internet there are millions of websites that our user base browse to everyday throughout the world. Our objective with Beulai is to provide a succinct and accurate summary of every site that our customer base visits for each site that has a EULA. Using advanced artificial intelligence and cutting-edge learning algorithms we will achieve seamless operation across multiple websites and platforms. To that end, we need to start by refining the accuracy of the summaries Beulai provides. With the initial goal of obtaining a 90% or greater accuracy in the EULA summaries we provide.

Key Result: Achieve a 90% accuracy rate in AI-generated summaries of EULAs.

Stakeholders: Beulai – Responsible for optimizing AI systems, ensuring data security, maintaining efficacy of systems as well as compliance with ethics, Users – Group using Beulai to optimize other platforms, Regulatory Bodies – Ensures compliance with laws to maintain privacy and ethical data usage

Beulai's user base is targeted towards websites and or businesses across widely different industries from media, news platforms, and e-commerce. Users' demographics represented by a wide demographic range across ages, incomes, and regions.

1.C.2.2 OKR 2 Metric(s) with Experiment(s)

Metric: Accuracy of AI-generated Summaries - Measure the percentage of AI-generated summaries that are deemed accurate by legal experts or a control group.

Experiment:

Setup:

Select a sample of EULAs

Use Beulai to generate summaries for each selected EULA.

Have a team of experts or users review the AI-generated summaries and evaluate for accuracy compared to the full text of the EULA.

Survey:

Create a survey for legal experts and reviewers to evaluate the accuracy of each AI-generated summary. With a focus on: Accuracy of the key legal clauses, Clarity of the summary compared to the original EULA, Comprehensiveness

Give users option to flag misleading or inaccurate generated summaries to notify us of the issue

Data Collection and Analysis:

Measure the summaries rated as "accurate" or "very accurate" by the reviewers.

Analyze the responses to calculate the percentage of AI summaries that meet the 90% accuracy target.

Adjustments:

If the accuracy is below 90%, identify patterns of errors or omissions and adjust the AI algorithm accordingly.

1.C.2.3 OKR 2 Ethical Impact(s)/Issues(s)

A potential ethical issue would involve data security and privacy concerns. With how we want for Beulai to function concerns regarding privacy arise considering it may require access to sensitive data such as browsing history or preferences. The matter of security also arises with how we want Beulai to track changes in EULAs and notifying our users which would need to involve storing data. Which would risk our user data leaking if not properly secured. This problem being exemplified by the case Google LLC v. Gonzalez which touches on issues of privacy and data collection.

Stakeholder Risks

Stakeholder	Financial	Privacy	Conflicting Interest	Violation of Rights
Customer	Low-none	High	Mid	High
Beulai	High	Low-none	Mid	Low-none
Regulatory Bodies	Low-none	Low-none	Mid	Low-none
Tech Companies	None	Low-none	Mid-high	Mid-low

Customer Stakeholder: The financial risks for users of our extension are low, as there's no direct correlation between extension usage and financial loss. Indirect impacts, however, could arise from either privacy breaches which may lead to increased costs over time. For privacy, the concern is invasion of privacy and or data collection. Users may not know when their data might be being collected potentially sensitive data that may impact the privacy of the user. Risk of conflicting interests is moderate. Our users desire a user-friendly system that clearly provides them a summarized EULA for websites they visit that isn't too intrusive. Providers may prioritize the company over users and their personal data. Balancing company interests with needs and wants of users with transparency is required to maintain trust. Risks for violation of rights remains high. This intersects with privacy risks as we have access to our user bases personal data there is a non-zero chance of their data being sold to data brokers and the like. This inherent risk leads to high chances of their personal data and their rights being violated.

Beulai Stakeholder: The financial risk for the company is high, as we may need to pay for access to advanced artificial intelligence and learning algorithms. Put together with needing to refine and iterate on those for a better product will lead to high costs. Privacy risks for the company remain low to non-existent. Risks of

conflicting interests is moderate. As providers may prioritize the company over the user base. Balance between company interests with user base is required. Risks for violation of rights remains low to non-existent.

Regulatory Bodies Stakeholder: Financial risk for regulatory bodies is low to non-existent. Privacy risk is low to non-existent. Risk of conflicting interests is moderate as they may be more concerned with ethics and customer rights rather than the company. Balance between ensuring company is acting within bounds and not acting with malicious intent to customers while also not hamstringing the company is advised. Risks for violation of rights remain low to nonexistent.

Tech Companies Stakeholder: Financial risk for tech companies is practically non-existent. Privacy risk is low to non-existent. Risks of conflicting interests with other tech companies range from moderate to high depending on the company that the AI summarizes the EULA from. The risks of violation of rights remain moderate to low.

1.C.2.4 OKR 2 Ethical Safeguards

1.   Transparency – To reduce the privacy risk of Beulai a proposed safeguard would be to be transparent and give informed consent to our user base before using our service [8]. Being informed on what data is collected, needed and how that data will be used and how long it will be stored as well as the ability for users to delete their data [9]. The groups involved in designing this safeguard would be legal experts such as lawyers or consultants, security and or data protection experts, and UI designers for the prompt. A way to measure this methods effectiveness is either through surveys and analytics or tracking how many users accept or decline the prompt.

2.   Compliance – To reduce risks of Beulai another safeguard would be to act with compliance and honor the data privacy standards set by CCPA and GDPR [10]. Groups involved would be an ethics board and or committee as well auditors. A way to measure effectiveness could be through analytics or through evaluations by an oversight committee to see if we are or aren't acting in compliance with data privacy standards.

3.   Protection – To reduce security and privacy risks of Beulai another safeguard would be to put systems in place specifically for data protection and security. Such as data resiliency, masking, erasure, and encryption [11]. Groups involved could be security experts, and data protection officers, and the like. A way to measure effectiveness could be through the hiring of white-hat hackers to test security measures put in place and see if they can or can't get the data.

1.C.3.1 OKR 3 Objective and Key Result

Beulai is to set a baseline of minimum daily users and grow by 15-25% over the next quarter. First, Beulai will identify the initial unique daily users baseline and then launch initiatives to grow it. This objective has a direct impact on various stakeholders, such as the businesses that are using Beulai's analytics, the end-users of the optimized platforms, regulatory bodies making sure that the project is compliant with privacy policies, and the internal development team of Beulai that is responsible for implementing tracking and observing ethical principles. Improved digital experiences are passed on to the end-users, while businesses derive higher engagement.

Nevertheless, issues such as data privacy, ethics, and compliance with the laws must be taken into consideration in order to maintain the sustainability and effectiveness of the growth strategy.

Key Result:

- Figure out the initial baseline of unique daily users.

- Then implement plans to enhance the minimum daily user count by 15-25% over the time frame.

Stakeholders:

- Businesses Using Beulai: These companies rely on Beulai's insights to increase their digital platform's engagement. They are affected by the accuracy and effectiveness of Beulai's analytics.

- End-Users: The individuals visiting the platforms optimized through Beulai. Their data is collected (anonymously) to improve engagement strategies.

- Regulatory Bodies (GDPR, CCPA): Ensure compliance with data protection laws to maintain user privacy and ethical data use.

- Beulai's Development Team: Responsible for implementing tracking, ensuring data security, and maintaining compliance with ethical standards.

Beulai's customer base has been targeted towards businesses across different industries such as e-commerce, media and SaaS platforms. End-users are represented by a wide demographic across different ages, incomes and geographical regions. Every business using Beulai's insights has to make sure that data collection and engagement strategies do not take advantage of or control vulnerable populations.

1.C.3.2 OKR 3 Metric(s) with Experiment(s)

Metrics:

- Unique daily users (measured using IP tracking and cookies for session identification).

- Daily traffic volume (total visits vs. unique users).

- Retention rate (percentage of users returning within a set timeframe).

Experiments:

1. Baseline Tracking: Track the activity of the unique IPs for the first time period (e.g., 30 days) to determine the current minimum daily users. (This enables better understanding of referral traffic behavior and optimizing strategy accordingly.)

2. A/B Testing on Landing Page: This makes it easier to determine what changes need to be made to the homepage to ensure that more people are engaged and are likely to convert.

3. User Engagement Initiatives: It also includes some features like personalize recommendations, push notifications, and incentives to increase the user return rates.

4. Referral Program: Develop and track the effectiveness of referral incentives that will encourage users to recruit new visitors.

1.C.3.3 OKR 3 Ethical Impact(s)/Issues(s)

Potential ethical concerns include:

1.   Privacy Concerns: Tracking user visits, even when anonymized, raises concerns about consent and data security.

2.   Accuracy & Bias: Users on shared networks may be miscounted, leading to inaccurate baselines or misleading insights.

3.   User Awareness: Lack of transparency about tracking methods may create distrust among users.

Real-World Case Reference:

The case of Google LLC v. Gonzalez touches on issues of user data collection and privacy. Google is under pressure over data retention policies and lack of transparency on user consent. The same concerns are possible for Beulai if its tracking practices are not explained well.

Stakeholder Risks

Stakeholder	Financial	Privacy	Conflicting Interest	Violation of Rights
Beulai	Mid	Mid	Low	Low
Customers	None	High	Mid	None
Tech Companies	Low	Mid	Mid	Low
Regulatory Agencies	Low	None	High	Mid

Customer Risk:

The financial and privacy risks that Beulai faces exist at a moderate level. The company needs to build secure data infrastructure and could experience negative reactions from customers when they view data practices as unethical. The pursuit of business objectives to boost user engagement creates ethical dilemmas regarding data management practices.

The tracking of behavioral data at an anonymized level makes privacy risk the highest concern for customers who are end-users. The financial exposure of customers remains zero but their rights face moderate risk because they lack knowledge about data collection activities or have not given consent.

The financial exposure of tech companies who work with Beulai remains low, but they must maintain equivalent privacy standards across their platforms. The failure to match ethical data practices between organizations would generate moderate conflicts between their interests.

The regulatory agencies face limited direct risk in their operations but they maintain responsibility to enforce compliance. The GDPR and CCPA regulations require regulatory agencies to step in when Beulai or its clients fail to comply with privacy laws.

1.C.3.4 OKR 3 Ethical Safeguards

Proposed Safeguards:

1. Anonymous & Aggregated Tracking: Make sure that no personally identifiable information (PII) is being gathered.

2. Privacy Policy Transparency: Explain how much tracking is going on and let users opt out of it.

3. Compliance with GDPR & CCPA: Honor global data privacy standards to steer clear of legal and moral consequences.

4. Ethical Oversight Committee: Create an internal review board, which may include ethical and legal consultants to review tracking mechanisms and user interaction.

Implementation Plan:

- Collaboration with Ethical Experts: In addition, work with privacy law specialists to develop data tracking policies.

- User Education & Awareness: Notify users clearly of tracking practices through clear notifications.

- Regular Ethical Audits: Perform regular evaluations to check that compliance with privacy laws is maintained.

- Measuring Effectiveness: Monitor user opt-in/out rates and study public sentiment through surveys. As for the tools, we'll use them to gather feedback, not to constant surveillance.

1.C.4.1 OKR 4 Objective and Key Result

Objective: Eventual 5% growth of revenue over costs.

Key Result: While we like to look at our service as doing good for the community, it is still important to cover our costs, and potentially make a profit. Our service could be considered a bit niche, so our expectations of revenue shouldn't be too high. Initial costs will be somewhat steep, and revenue will be at its lowest for when our service is implemented, so a negative loss is to be expected in the first year or so. Key stakeholders will be our Beulai company, as we care about running the service at a profit, and our clients, who care about the continuous service to keep them up to date to the ever changing EULAs of the many websites they will seek to interact with.

1.C.4.2 OKR 4 Metric(s) with Experiment(s)

We have two metrics to keep track of: costs and revenue, which will be calculated in United States Dollar.

For costs, there are a few things to track:

1. Development: The development of our AI model responsible for summarizing, data scraping method, our website, and website extensions, is expected to initially cost up to $50,000.

2. Maintenance: The hosting of our website, servers, and storage costs is expected to cost about $1,000 monthly. Our web scraper is expected to cost up to $15,000 annually.

3. Legal teams: While we ideally would not have to worry about being sued, it is important to set aside some money just in case. We could set aside $10,000 to use for legal teams, on a need to need basis.

For a summary of the expected costs of our first year of running the service, it is expected to be around $100,000, with an expectation that costs would reduce significantly in the following years, down to around $35,000 annually.

There are a few ways we can go about generating revenue:

1. Advertisement: An easy way would be to use un-personalized advertisement on our website, using affiliate marketing and sponsored content, which could generate up to $15,000 annually, if given a decent amount of monthly traffic.

2. Freemium: We could run the service with a freemium model, being free to users who just want to check a few sites, and asking a price for those, especially big companies, that want to learn more about the EULAs of most of the significant websites out there. We could charge $1,000 on a monthly basis for unlimited usage, which could generate revenue of about $20,000 annually.

3. Donations: Considering we are doing a good service for the privacy-oriented community, we could ask for donations to help cover costs. We could expect at least $2,500 annually.

For a summary of expected revenue, we could expect at least $37,500, with our revenue being half that for the first year. Profit for the first year would be a negative $60,000, taking into account initial development

and low revenue due to low popularity. I would expect a profit of around $2,500 for the 2nd year, no longer having to worry about initial costs, with expectations that our revenue and profit would steadily increase as the years went by, as our site got more popular and lucrative.

1.C.4.3 OKR 4 Ethical Impact(s)/Issues(s)

Considering we provide a service of checking and providing summaries of EULAs, it is paramount that we maintain a good reputation, as our clients will lean heavily on the side of being privacy oriented. We must cater to such a mindset, regardless of how difficult it may be for us to make profits. For example, many websites love to take data from the user, whether secretly or not, and use that to profit from being a data broker. There might be a desire to do that in our company, if the profits aren't coming in, but not only would that be immoral, it would potentially ruin our reputation and profits in the long run. Privacy for the individual is a very significant issue in today's environment, and we care that we don't contribute to any negativity. It is also important to keep in mind the privacy of companies, but it isn't such a strict issue as with the individual, and it definitely isn't as much of an issue in our case, since we are dealing with publicly accessible EULAs.

Stakeholder Risks

Stakeholder	Financial	Privacy	Conflicting Interest	Violation of Rights
Beulai	Low	Low	Medium	Low
Customers	Low	Medium	Low	Low
Tech Companies	High	High	High	High
Regulatory Agencies	Low	Low	Low	Low

As Beulai, we are not at too much financial risk. The runtime for our service is expected to be low, and we do not expect too much profitability. Worst case scenario, we do not gain anything from the little costs to run our service. We might have a privacy risk if we make our code open-source, opening ourselves up to having our work stolen, but other than that, it would be a non-problem. We might have somewhat of a conflict of interest, as we are scraping the internet, more in particular major sites and companies, of their EULA, which would give us data that we could use to better compete with such companies. We obviously do not pose a violation of rights against ourselves.

As for the client, there is little financial risk. How much they decide to put into our service would be completely voluntary, including none, if they so wish. Just like when using any online service, there is a privacy risk for people to worry about, but with the way we are handling our service, they would only have to worry about the risks of creating an account with us, and any payment methods they might use. As for conflicting interests, there isn't much our clients would feel to care much about, especially since they aren't involved in the process of scrapping EULAs. Besides privacy rights, our clients don't really have to worry about any other rights being violated, as it is not in the scope of how we operate.

For the tech companies and all the websites whose EULA we scrape, they could have a high financial risk from what we do. With the information of EULAs we give to our clients, our clients would be able to better know what kind of terms they are agreeing to, possibly influencing them to change what online services they use. Our service would be promoting better competition, as our clients know more to be able to compare companies EULAs. This would especially negatively affect companies with malicious EULAs, like those that are particularly privacy invasive.

For regulatory agencies, there is virtually no stake to have in our company.

It could also be argued that tech companies have a high privacy risk from our service. When our service scrapes a website's data for its EULA, it could be considered stealing intellectual property. Another problem is what we do with that data, like how we store and distribute it.

Tech companies also have a big conflict of interest, as just like previously mentioned, we promote competition by informing our customers to make more informed decisions on what online services they want to use. Another concern is how our service represents a website's EULA, like if it would leave things out or misrepresent wording, especially since it is a legal document, possibly raising issues with legality, regulations, copyright, and misinformation.

To assure our stakeholders that we won't face a premature shutdown due to legal issues, we can talk about web scraping. A case that supports our case of web scraping is the case hiQ Labs v. LinkedIn, where it was ruled that hiQ should be allowed to scrape public data from LinkedIn, especially as it was supportive of antitrust laws, and that the scraping did not violate the Computer Fraud and Abuse Act [12].

1.C.4.4 OKR 4 Ethical Safeguards

1. With our services, we plan to mitigate how much we intrude on the privacy of the clients as much as possible. When the client uses our service, we do not take any data from the user that could be potentially abused, except when creating an account and doing payments. We can ensure data security and privacy through many different ways: 1. We can obtain an SSL certificate to ensure proper data encryption between our website and our clients. This is an absolute must for data security. A case that highlights this being important is the Target data breach in 2013, where hackers were able to get the financial data of 40 million customers, due to faulty encryption of communications between Target and their customers [13].

2. We can make use of multi-authentication for those that create an account, which helps a lot with account security. We can consult cybersecurity experts to implement and maintain such systems, and anything similar.

3. We can ensure compliance with the General Data Protection Regulation and California Consumer Privacy Act, two significant comprehensive data privacy laws, to not only ensure legal compliance, but to ensure a level of protection of privacy, as accepted by the government. We can use the help of legal experts that are well versed with such laws. It would be easy to measure the effectiveness of our compliance by not just getting feedback from legal experts, but by looking at how often we are sued. Being sued and losing would not only potentially force us to shut down our service, but it would be a huge financial loss, cutting down any profits we may have made. An example of a case of not complying with privacy laws, more in particular the GDPR, is the GDPR enforcement against Google, where France fined Google 50 million Euros for not being transparent about how they collected data [14].

4. We can partner with 3rd parties such as Paypal to securely handle payment methods, so we don't have to worry about getting and protecting the data ourselves. As for our service itself, the best way we could put in a safeguard against malicious programming is to make our code partially or fully open-source, allowing anyone to check its code to confirm it conforms to our own EULA, and that there isn't anything malicious. An open-source service could potentially be taken advantage of, but it might still be worth doing.

2: Cultural Policy

2.A. Core Values

At Beulai, the core values are rooted in integrity, innovation, and responsibility. We want to be considered a company that pioneers cutting-edge technology and stands firm in its commitment to ethical practices. We believe that technology should be a force for good—transparent, inclusive, and sustainable. We prioritize user trust and data privacy in everything we build. From our algorithms to our user interfaces, we design with the user in mind, ensuring that our systems serve people, not just business goals.

We value collaboration across teams and with our clients. Open communication, active listening, and mutual respect are the foundation of our relationships. Every voice matters—whether it's from our engineers, our clients, or the users whose data we are trusted with. We encourage creativity, learning, and a healthy questioning of assumptions to drive innovation. Excellence at Beulai is not just about technical brilliance; it's about how we apply that brilliance to solve real problems in responsible and impactful ways.

2.B. Motivation

At Beulai, we love building tools that make people's lives better. We are inspired by the potential of data to illuminate, improve, and transform digital experiences. What excites us most is creating solutions that help businesses grow while respecting user privacy. We are driven by curiosity, fueled by data, and guided by empathy. We love seeing our work lead to positive outcomes—whether that's a small startup doubling its engagement or a large organization finding more meaningful ways to connect with its users.

But we also have our fears. We fear becoming disconnected from the people we serve—the users behind the data. We are wary of losing transparency or becoming complacent with ethical shortcuts in pursuit of performance. We fear contributing to a digital world that's optimized for profit but not for people. These fears keep us grounded and reinforce our mission to lead with responsibility and integrity in everything we do.

2.C. Summary

Ethical Innovation, User-First, Transparent Always.

3 : Ethics Policy

3.A Core Items:

Privacy

As our most important policy we dedicated most of our systems with privacy in mind, as well as deeply invested in mitigating any risks in our user's privacy. Beulai as the current version permits doesn't store any user data or personal information, as well as not requiring any login credentials.

Responsibility

As AI is a rapidly evolving technology still in its early stages, with emerging risks and increasing complexity, we implement rigorous testing, oversight, and constant diligence to ensure the safety and confidence of our users.

Explainability

Due to the nature of AI, we endeavor to help users understand how our AI application operates, as well as set clear disclaimers to set clear expectations with our product – such as reminders that the AI-generated outputs may contain inaccuracies.

Transparency

Over time, we will build up a history of the EULA's and term of services from different websites. We will also generate summaries for each of these agreements. All documents will be freely accessible to the public for review. Users can suggest changes, and version control will allow anyone to compare changes that are made from one version to another.

3.B Board:

Orin Kerr: is an American legal scholar and professor of law at the UC Berkeley School of Law known for his studies in American criminal procedures. He is an expert in the U.S Constitution, specifically concerning Fourth Amendment issues focusing on privacy rights. He is also known for his knowledge of computer crime law, internet surveillance, and online privacy law. He advocates for end-users, asserting their right to a reasonable expectation of privacy when sharing information with online service providers. He was chosen because fir his legal pedigree, especially concerning the Fourth Amendment and privacy issues, especially related to online interactions and criminal activity.

Tim Berners-Lee: is an accomplished computer scientist with a lot of awards under his belt such as Queen Elizabeth Prize for Engineering, and the Association for Computing Machinery's Turing Award, and much more. He is best known for being the inventor of the World Wide Web, The HTML markup language, the URL system, and HTTP. As well as a professorial research fellow at the University of Oxford and a professor

emeritus at the Massachusetts Institute of Technology. He is an ardent supporter of users rights online, arguing that internet access is a human right, internet traffic should be neutral and not subject to throttling by internet services providers (Net Neutrality), and that user's privacy should be protected. He created "Solid" (SOcial LInked Data) in 2016 to help give end users control of their data and who has access to it. He was chosen both for his experience and knowledge of the Internet as well as being a major advocate for privacy and Internet anonymity.

Timnit Gebru: is a computer scientist who works in the fields of artificial intelligence, algorithmic bias and data mining and is the founder of the Distributed Artificial Intelligence Research. She is best known for being fired from Google for her contributions to a paper as co-lead of the Ethical Artificial Intelligence Team that discussed the risks of large language models without waiting for an internal review by Google. She was chosen for her expertise in both the inner works of AI development as well as in the ethics of artificial intelligence.

5 : References

[1]   T. Clayburn, "Lawmakers propose TLDR Act because no one reads Terms of Service agreements," *The Register*, Jan. 14, 2022. https://www.theregister.com/AMP/2022/01/14/tldr_act_terms/

[2]   E. Weise, "Amazon wrote a zombie apocalypse clause into its terms of service and here's why," *USA Today,* Feb. 10, 2016. https://www.usatoday.com/story/tech/news/2016/02/10/amazon-adds-zombie-apocalypse-disclaimer-new-video-game-engine-terms/80183780/

[3]   H. Murphy, "WhatsApp fights back as users flee to Signal and Telegram," *Financial Times,* Jan. 13, 2021. https://www.ft.com/content/ee1b716d-4ed2-4b26-8da1-40c98db7b9b6

[4]   N. Chokshi, "Terms of Abuse: Reading the Fine Print," *The Atlantic,* Apr. 19, 2010. https://www.theatlantic.com/technology/archive/2010/04/terms-of-abuse-reading-the-fine-print/39086/

[5]   C. Cakebread, "You're not alone, no one reads terms of service agreements," *Business Insider*, Nov. 15, 2017. https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11

[6]   V. Allen, "The Limitations of Applying the Stored Communications Act to Social Media," *Southern California Law Review, Vol. 96, No. 3,* July, 2023 https://southerncalifornialawreview.com/2023/07/23/the-limitations-of-applying-the-stored-communications-act-to-social-media/

[7]   P Schrodt, "Edward Snowden just made an impassioned argument for why privacy is the most important right," *Business Insider*, Sept. 15, 2016. https://www.businessinsider.com/edward-snowden-privacy-argument-2016-9?op=1

[8]   IBM, "Ai ethics," *Ibm.com*, Sep. 17, 2021. https://www.ibm.com/think/topics/ai-ethics

[9]   State of California Department of Justice, "California Consumer Privacy Act (CCPA)," State of California - Department of Justice - Office of the Attorney General,2024. https://oag.ca.gov/privacy/ccpa

[10]   European Commission , "Data protection," commission.europa.eu, 2023. https://commission.europa.eu/law/law-topic/data-protection_en

[11] IBM, "Data Security," *Ibm.com*, Jun. 11, 2021. https://www.ibm.com/think/topics/datasecurity

[12] "HiQ Labs v. LinkedIn Corp. - Global Freedom of Expression," *Global Freedom of Expression,* Oct. 29, 2023. https://globalfreedomofexpression.columbia.edu/cases/hiq-labs-v-linkedin/ (accessed Mar. 12, 2025).

[13] C. Jones, "Warnings (& Lessons) of the 2013 Target Data Breach," *Red River*, Oct. 26, 2021. https://redriver.com/security/target-data-breach

[14] C. Ward, "GDPR Enforcement: How the 2019 Google Fine Made a Statement," Digital Marketing Institute, Mar. 04, 2019. https://digitalmarketinginstitute.com/blog/gdpr-enforcement-how-the-recent-googl e-fine-makes-a-statement