1. Ethical Business Plan

1.A. Company Name: Crime Data Inc.

1.B. Long-Term Vision Statement

1.B.1 Goals:

At CrimeData Inc. we aim to pioneer public safety giving law enforcement the tools they need to prevent crime before it happens. By leveraging big data and AI, we enable cities to be proactive instead of reactive. CrimeData Inc. is a cutting-edge analytic company with the goal of making cities safer through real-time data analysis and predictive policing.

1.B.2 Idea Origination:

CrimeData Inc. started with a realization: crime prevention needed to evolve. While studying computer science our team noticed that police departments often rely on outdated, reactive methods. We saw an opportunity to use AI and big data to bring law enforcement into the future. We wanted to be at the forefront of the AI boom and bring to market a product that would gain favor for AI by the public.

1.B.3 Purpose/Values/Mission:

The mission and duty of Crime Data Inc is the mitigation of crime through systematic and prevention of harm to the residents in the communities that our tools are used in. Our goal over time is to deter future crime through the effectiveness of our products such that criminals dare not linger in communities that utilize Crime Data Inc.

1.B.4 Key Questions:

i. How will we ensure transparency with shareholders?
To maintain the utmost level of transparency we will form a council of customer cities that will have permission to audit the entirety of the company during the annual report filing and will have a chance to share their findings with the shareholders. We believe that this committee will prove our commitment to engagement in transparency and

ii. How will we effectively use AI to increase policing efficiency?
The use of generative AI will allow our customers and systems to offload repetitive tasks to focus on adding maximum value to the communities that we wish to serve. Tasks that take away valuable time such as paperwork and other administrative tasks

iii. How will we reduce unfair biases in the products and services we provide?
The method our startup uses to reduce unfair bias in our products and services is to create accountability algorithms and systems. In our algorithms we have built in abuse detection as well as trustworthy third party auditing to make sure we utilize the best practices available. Aside from technical expertise we make sure to incorporate community input into how we can make our product more reliable and safer.

1.C.1.1

Our goal is to improve the response times of the police by 15% within the first year. As more local governments join us on our mission, our databases improve. AI refinements and gathering feedback from law enforcement will ensure the model's accuracy in identifying high-risk areas gets more accurate.

Some of our stakeholders include Law enforcement, residents, and the local government. Local government is an important stakeholder as it provides funding for our mission. They will also assist us with oversight so we can build a trusting relationship between us and the data they provide. Law enforcement is another group of stakeholders. They will be the ones using our service. This will be using the predictive patrols and will help us gather more data such as response time and active crimes. Lastly, the residents. They are the ones that can be affected by the predictive crimes. If not properly implemented they could be potential victims of over-policing and privacy violations.

We plan to lower our law enforcement's response time by optimizing the patrol routes and providing real-time incident updates. Achieving these outcomes will demonstrate the effectiveness of our predictive algorithm and help secure more support from all our shareholders.

1.C.1.2

To hit these goals we are looking to do the following

- Track and compare average response times before and after the implementation of our predictive patrol routes
- Increase real-time communication between law enforcement and our system to be integrated with current incident reports
- Improve predictive accuracy of identifying high-risk areas through model refinements and data gathering.

To these issues, we would conduct an experiment comparing police response times before and after going through our implementation of the AI model. The goal of this is to determine if our program makes any measurable difference in response times.

We would start by collecting data. We would gather historical data on police response and when the dispatch call went out. Higher priority incidents such as assaults or robberies would be weighted higher. This would be our baseline time.

We would then integrate our AI model and test it for an initial 6 months. During this time it will recommend patrol routes to follow. Over this time the model will back itself data to find any optimizations during these months.

After the 6 months are over we will revisit the data and response time to see if there are any significant changes in time. We will compare the average response time and find any correlations between the increased patrol efficiency and our system.

The expected outcome would be a measurable decrease in average response time to high-priority incidents by at least 15%.

1.C.1.3

One ethical impact would be the potential data privacy concerns of a private company storing all these personal data. This could be a concern as the public never had an opportunity to consent to being policed this way. Privacy is a big concern for us. Facebook was part of a class action lawsuit *Patel v. Facebook*. In this case, it was ruled that the collection of biometric data was a violation of the "Biometric Information Privacy Act (BIPA)." in the state of Illinois [1]. We will have multiple safeguards and transparency to avoid being put in the same situation as Facebook.

Stakeholder	Financial Risk	Privacy Risk
Law Enforcement	low	mid
Resident	low	high
Local Government	high	low

Law Enforcement: The financial risks for law enforcement are low, as they do not pay for our service. However, there may be a privacy concern. Since we want to optimize routes and response time, it would be important to have their real-time location. This could mean their sense of privacy could be seen as invaded, but our transparency and their expectation of being on the job leads it to be not a high risk.

Residents: The financial risk for residents is low as they are not paying for the service. However, privacy risks are high because increased police presence in certain areas may lead to over-policing or discriminatory targeting. Residents may feel as though they are under constant surveillance, raising concerns about their privacy and civil liberties

Local Government: The financial risk for local government is high as they are funding CrimeData Inc. The return on investment must be evident to justify continued funding. Privacy risks, however, are low as the government's involvement is mainly administrative and policy-driven. Their primary concern will be ensuring that the collected data does not lead to legal issues or public distrust. To mitigate financial risk, we will provide quarterly impact reports demonstrating reduced crime rates, improved response times, and increased public satisfaction.

1.C.1.4

One of the safeguards we have is anonymizing the data we collect. For the privacy of the residents, our data will not track any identifiers such as names, faces, gender, etc. This is to prevent any racial bias or discrimination that could come up as an ethical concern. All the incoming data will be stripped of personal identifiers before being analyzed. This will be effective to build trust with the public and fight any privacy concerns. Although this cannot be measured we will be under constant 3rd party watch. We allow the local government that we are working with the review any of our systems to be transparent to all of our shareholders.

Avoiding collecting any identifiers creates safeguards from being in the same situation as Facebook. Anonymizing data is an effective way to get data without privacy concerns. For example, Uber Movement is an initiative by Uber that collects and anonymizes data from millions of Uber trips [2]. This data was used for insights into traffic patterns and travel times in cities worldwide. This was used by urban planners and researchers to help make informed decisions about infrastructure and transportation.

1.C.2.1

CrimeData Inc. strives for transparency and trust in its use of AI and storage of data. In our annual reports, we aim to be upfront about the data we collect and use in each crime, as we understand the need for honesty in today's digital world. Each report will detail how our technology contributed to the outcomes of crimes contained in public records, expand on our partnerships with various government entities, and reassure the public of the select few who have access to their data. With this measure, we hope to reduce complaints by those who understandably care deeply about privacy, and how easily it can be abused.

Key stakeholders include our company, our partners in government agencies and local law enforcement, and the citizens of those in communities that have implemented our product. Our company, of course, will provide the servers and databases required to use our product in the cities it is needed in, and guide our customers through the implementation and maintenance of our product. If we fail to provide the proper service, our sales would be affected greatly, so we strive for customer satisfaction. Government and their law enforcement who use our product will provide support and guide us on how our product can best suit their needs. Their income will benefit the company greatly. Finally, residents and people who live in the communities where our product will be implemented are most important. We will ensure that their safety comes first, as they are the ones who will benefit the most from the use of our product.

1.C.2.2

With our goal of trust and transparency, we will measure this by a lowering percentage of complaints in regards to privacy in the use of our product. We will provide the opportunity to send in complaints either through the government agency using our product or through us directly, whether online, on the phone, or by mail. Using the number of complaints after the first year of implementation as our starting point, we plan to analyze the change in complaints in the years following.

The complaint will gather the information using the list detailed below, but not limited to, from the complainant:

- Identifying information (such as address, contact, name, etc) of the complainant
- The city law enforcement they come under
- Whether the complaint involves them or not; if not, their relation to whoever does
- Any incidents they have been involved (so we may determine their relationship to the use of our product)
- How they may be contacted for further information
- How they would like to send their complaint (online, phone, mail)

Afterwards, they will be further prompted to provide the specifics of their complaint in regards to privacy violations. Finally, we will ask any further questions, and accept the report.

We aim for a 20% reduction in complaints each year. By analyzing the main complaints of privacy, we will be able to reassure complainants about any violations, perceived or otherwise, that our company is involved in. Through this method, we can tailor our policies and reports to better reflect the needs of the public.

1.C.2.3

There are many ethical impacts and issues associated with our product, especially since it handles important, confidential data.

Expected Ethical Impact Risk Table

Stakeholder	Financial	Privacy	Conflicting Interest	Violation of Rights
Company	Mid	Low	High	Mid
Government/Law enforcement (customers)	Low	Low	Low	High
Citizens/General Public	Low	High	Mid	Mid

Analysis of Ethical Impact Risk:

Citizens/General Public: They have a low financial risk, as there is not much financial loss associated with their relationship to this product, as it is just their data being collected. However, they do have a high privacy risk, as much information about them is being recorded and stored with the Gov using the product's databases. The violation of their privacy either by hackers or law enforcement can greatly affect their life, as they may be arrested or accused of a crime, dragging them into a lawsuit. Additionally, there is a medium conflict of interest because citizens would want their privacy, but must understand that law enforcement will always need certain information in order to solve and prevent crime, and there may always be a struggle between the two. Finally, there is a high violation of rights. As stated before, it can allow for an abuse of power by law enforcement and the government, along with data leaks also by the company, greatly impacting the privacy and safety of citizens. Even if just a data leak happened, "At the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice," and have enough of a serious impact on citizens [1].

Government/Law Enforcement: They have a low financial risk mainly because there is nothing the general public can easily do if the Gov has ethical issues. The Gov agency and law enforcement will likely continue to receive funding despite the ethical issues. The risk of privacy impact is also low because the Gov is good at keeping information about itself confidential. However, conflicting interests may be low because the government is in need of a product like this, and the company is happy to provide services for them as they are paying customers. Finally, the violation of rights is high. The product can easily be used to justify actions taken by law enforcement that are not in accordance with the law, or skip procedure on the basis that the AI is correct. This is a major issue that would affect everyone involved with the product negatively, as it would put mistrust on the product and the government.

Company Stakeholder: There is a medium risk financially for the company stakeholder, as while there are not many direct ethical issues that would cost money for the company, the reputation of the company may be tarnished with ethical issues if too many occur, leading to decreased profits over time and less people willing to take our product. For privacy, it is a low risk for the company as the only information it has to lose is the list of customers and the AI technology, which is not much for ethical impacts. For conflicting interests, it is high because the company may offer to violate privacy rights and such of the data it collects when faced with a larger payout from customers. Finally, the violation of rights is high because it needs to make sure that it is not liable to lawsuits against privacy. For example, the class action lawsuit Patel v. Facebook occurred because Facebook did not inform its users of using their data and how they did so, leading to the entire class action lawsuit [1]. A simple notification of how Facebook was going to use the data would have been sufficient to circumvent the whole thing.

1.C.2.4

For this OKR, the main safeguard is there to protect the privacy of citizens in cities that use the product. Transparent Data Encryption of all the data that is collected by the company's product is an ideal way to ensure privacy and dissuade violations, as it also safeguards against the abuse of data by those authorized to view it [3]. Additionally, we will have strict control of whoever can directly access the data, and only allow for the sharing of data between cities and governments with express permission from both sides.

We will consult security and encryption experts through trusted third party companies to design and implement such services. We will also use our own experts to ensure the third parties do not take advantage of any access to the data. In general, any data collected in the system will be automatically encrypted, with only the AI model allowed access at any time. Any other time, we will have an electronic system that records any person and device that asks for access to data that is unencrypted.

The only drawbacks is that it would be hard to measure the effectiveness. Any data that had gone out may be hard to realize at first, but it means that we would be able to narrow down the suspects easily without fail, as we have records of whoever could access that data. Thus, we hope to reassure citizens and law enforcement that their data is safe and they do not have to worry very much about it.

1.C.3.1

Due to the sensitive political nature of crime and policing Crime Data inc must make sure for ethical and compliance reasons that city customers are not racially profiling residents with our software. Our goal is to ensure crime risk assessments that do not have racial bias because the consequences of not purposefully addressing this issue before mass adoption of our software product are dire. Firstly aside from just legal repercussions significant population backlash could cause the elected officials comprising the city councils which are our main customers to be replaced via election thereby ending our revenue stream from said city. As faithful stewards of a powerful technology the goals of fairness towards the community and safety are not mutually exclusive therefore it is possible with the proper technical solutions a non biased crime assessment through our solution. Statistically speaking young men that are unemployed are significantly more likely than other demographics to pursue criminal activity if for nothing else than for economic gain[5]. Given the complex dynamics of crime in communities and who is more likely to commit it the possibility for bias on the basis of not just race but gender and age could be rampant within our software if safeguards are not implemented.

1.C.3.2

Fundamentally as a product provider the most key metric in relation to product and the goal to diminish bias in crime assessment is community involvement. The first experiment after a pilot is conducted in the customer city is to do a survey regarding the pilot. We believe its important to have feedback from the people that have the most ethical risk imposed upon them through the use of our software tools. This data collected will be a simple random sample and the first question it would ask is ”Do you believe unjust arrests have happened because of Crime Data Inc.” As well as ”Do you believe that Crime Data Inc is having a positive effect in your community Yes or No” for this survey we plan to use the best methodologies available to reduce sampling error as discussed in [6]. The specific two questions we have chosen for our survey are about measuring the likelihood that a discontent resident would likely politicize the city’s usage of the software. Which is to say if the negative reaction is high enough as possibly indicated by the survey it could possibly mean community activism to revoke our license to operate.

Aside from this general survey metric another metric we also wish to keep track of is the number of arrests associated with opportunity zones. Opportunity zones are a federal designation given to localities or zip-codes which meet a certain level of economic disenfranchisement to qualify for federal grants and other economic incentives. Opportunity zones as a term is simply a friendlier designation for economically deprived area in need of investment. The metric we specifically care about to see if certain sections of the community are being targeted is the weighted average of arrests in wealthy zip-codes in the city compared to the opportunity zones. If from this method we see a significant skew with arrests in opportunity zones this will warrant further investigation to prevent biased crime assessment.

1.C.3.3

With the wide ranging impact and stakeholders that Crime Data inc must be in communication with we created an ethical risk table to better understand the demographics and stakeholders our technology poses a risk to.

Stakeholder	Financial Risk	Privacy Risk	Conflicting Interest Risk
City Customer	Mid	Low	High
Residents	Mid	High	Low
Company	High	Low	Low

Table 1: Expected Ethical Impact Risk Table

Based on this ethical risk its clear to see that the highest level of financial risk posed by lawsuits is the company while the city customer would bear some as well as the executor of the program. The mid-level of financial risk posed to the residents is from the possibility of wrongful arrest thereby requiring an attorney and the associated legal fees. The greatest privacy risk being born by the city residents bears extreme ethical impact. This is because residents data is being harvested and used by our software product and this can possibly also lead to wrongful arrest as mentioned previously. Although this risk is high the outcome of a data leak or breach is very low because all data is stored locally with the city customer. The biggest ethical risk that is visible to see is the conflict of interest. This is because the lawyers responsible for trying criminals caught by our system work for the district attorney's office and therefore have a close link to the city. Although the law accounts for this through the criterion for admissible evidence this asymmetry of information is still important to point out. In the case of Herrera v. Raoul the conflict of interest in the usage of heat maps as probable cause was an issue investigated by the court because it would mean any arrest could be validated with predictive policing. This further exemplifies why conflict of interest is an active issue in predictive policing.

1.C.3.4

Simply due to staffing and volume practicalities Crime data cannot investigate every single suspected abuse of our software that violates our user agreement and ethics. For this we have created a multi step plan to deal with and filter only the most serious cases directly with our staff.

1) Implement and publicly document bias mitigation strategies in the algorithm, with third-party audits twice a year.

To best identify and track improper use of our software we are implementing an experimental algorithm which will analyze each and every query to our server. For the sake of transparency we will conduct audits by a third party trusted service of the customer's choosing. With that said the parameters of the algorithm must be kept secret to prevent cities from gaming the algorithm and thereby bypassing the safeguards. The first parameter of our algorithm uses location radius of interest that is used by the customer city when it is querying our server. Generally speaking we advise customers to not look at ratings by zip code but rather passive results that the software provides that will be fed into police systems. If a customer is constantly querying a specific block or neighborhood this would be a red-flag warranting further investigation. For the audit we plan to engage a firm or expert consultant who is either of the community or at the very least someone trusted by the community.

2) Maintain a false positive rate for high-risk classifications below 10% when controlling for racial bias factors.

This safeguard must be implemented at the software logic level. As a technical problem, maintaining a false positive rate for high risk classification requires a machine learning classification model. This classifier must assess for and recognize high risk populations and model them as a proportional of total assessments. Our engineering team will create a model architecture to implement this into our application. The model will be continuously trained until the error rate is satisfied.

3) Conclusive evaluation of the experiment

To conclude our evaluation of the algorithm experiment we will establish an expert panel of roughly five esteemed individuals in their fields of study. The first member will most certainly be a lawyer given the requirements of compliance to prevent lawsuits. The second expert we plan to incorporate into our panel is a pastor from the community. Though this may be a bit unorthodox, having an expert of religious ethics and morals will be a valuable asset in this evaluation. The rest of the panel will consist of mathematicians and computer scientists to evaluate on an objective technical basis the efficacy of the experimental algorithm. The Belmont report which serves as the basis to form this panel advocates for diverse perspectives when dealing with ethical issues[8].

References

[1]"UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT." Accessed: Mar. 7, 2025. [Online]. Available: https://epic.org/wp-content/uploads/amicus/bipa/patel-v-facebook/Patel-v-FB-9th-Cir-Opinion.pdf

[2] Uber Technologies, Inc., "Visualizing Traffic Safety with Uber Movement Data and Kepler.gl," Uber Blog, May 17, 2019. [Online]. Available: https://www.uber.com/blog/kepler-data-visualization-traffic-safety/. [Accessed: Mar. 7, 2025]

[3] V. Shaik and Dr. N. K, "Flexible and cost-effective cryptographic encryption algorithm for securing unencrypted database files at rest and in transit," MethodsX, vol. 9, p. 101924, 2022, doi: https://doi.org/10.1016/j.mex.2022.101924.

[4] Association for Computing Machinery, ”ACM Code of Ethics and Professional Conduct”, Association for Computing Machinery. [Online]. Available: https://www.acm.org/binaries/content/assets/about/acm-code-of-ethics-booklet.pdf. [Accessed: Oct. 26, 2023].

[5] RAND, ”More Than Half of Unemployed Young Men Have Criminal Records; Findings Suggested New Approach Needed to Aid the Unemployed," RAND, [Online]. Available: https://www.rand.org/news/press/2023/11/08.html. [Accessed: Dec. 15, 2023].

[6] J. Ponto, ”Understanding and evaluating survey research," J. Adv. Pract. Oncol., vol. 6, no. 2, pp. 168-171, Mar.-Apr. 2015, Epub Mar. 1, 2015. [PMID: 26649250; PMCID: PMC4601897].

[7] Herrera v. Raoul, No. 23-1793, United States Court of Appeals for the Seventh Circuit, 2023.

[8] The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research, U.S. Government Printing Office, 1979.