OpenMined is an open-source community focused on researching, developing, and elevating tools for secure, privacy-preserving, value-aligned artificial intelligence.
Key Activities

◆ **Awareness:** Raise awareness of Secure, Private, & Value Aligned AI

◆ **Tools:** Lower the barrier-to-entry by building open-source tools

◆ **Community:** We have really fun Hackathons…
Outline

- **Why**: the AI Business Model has privacy problems
- **How**: an Introduction to the Core Technologies of OpenMined
  - Federated Learning
  - Homomorphic Encryption
  - Multi-Party Computation
  - Gradient Marketplace
- **Roadmap & Demos**
1. Acquire Data about People

The AI Business Model
2. Train a model that transforms one dataset into another
3. Sell the Use of that Model
Step 1: Acquire Data about people

Step 2: Train a Model that predicts unknown facts about a person using known facts.

Step 3: Sell the Use of that Model (the App)
Problems with the AI Business Model

◆ Step 1: acquire **Data** about people
  - **Privacy**: people lose control of their data
  - “**Sensitive Products**” don’t get made
**Problems**

- **Step 2**: train a **Model** that predicts unknown facts about a person using known facts.

  - **Contagious Privacy Loss**: if one person reveals private information, AI can be used to reveal private information of others through prediction.

  - **Lack of Competition**: there is very little market competition because most datasets are proprietary. (AI Inc. vs AI Corp.)

  - **Unfair Predictions**: corporate datasets only sample the target market (customers) of the company that acquired them, leading to biased AI predictions.
Problems

◆ Step 3: sell the use of that Model (The App)

- **Lost Natural Income**: in practice, people are rarely compensated for their data
- **Unknown Value of Data**: How valuable is any datapoint?
- **Unknown Accuracy of Predictions**: the quality of deployed models is unknown
- **Digital Assets Hard to Protect**: (i.e., pirated music)
How do we solve these problems?
Potential Solution

- **Train** A.I. on data we cannot see
  - **Privacy Win:** people wouldn’t need to reveal their data
Outline

- **Why:** the AI Business Model has privacy problems

- **How:** an Introduction to the Core Technologies of OpenMined
  - Federated Learning
  - Homomorphic Encryption
  - Multi-Party Computation
  - Gradient Marketplace

- **Roadmap & Demos**
Introduction to Federated Learning for Safe AI
Non-Federated Learning

AI Inc.

Model

Jane's Data
Jack's Data
Joe's Data

Federated Learning for Safe AI
Federated Learning for Safe AI

Jane's Data
Jack's Data
Joe's Data

AI Inc.

INITIAL Model
Federated Learning for Safe AI
Federated Learning for Safe AI
Federated Learning for Safe AI
Federated Learning for Safe AI
Federated Learning for Safe AI
Open Source

- TensorFlow
  - Computer Cluster
  - Parameter Server

- OpenMined
  - Federated Learning
  - Blockchain Compute Grid

Federated Learning for Safe AI
Potential Solution

- **Train** A.I. on data we cannot see - Federated Learning
  - **Pro:** the data is kept private
  - **Theft:** the A.I. is put at risk.
  - **Privacy:** Gradients reveal information about the data
  - **Sensitive Product Problem**
Potential Solution

- **Train** A.I. on data we cannot see **without revealing the AI or its training updates to anyone?**
Potential Solution

- **Train** A.I. on data we cannot see without revealing the AI or its training updates to anyone?
  - Homomorphic Encryption
  - Multi-Party Computation
Introduction to Homomorphic Encryption for Safe AI
Homomorphic Encryption

3 ➔ Homomorphic Encryptor ➔ Cypher A
0010110101

Homomorphic Encryption for Safe AI
Homomorphic Encryption

3 → Homomorphic Encryptor → Cypher A
   0010110101

5 → Homomorphic Encryptor → Cypher B
   100100110
Homomorphic Encryption

3 $\rightarrow$ Homomorphic Encryptor $\rightarrow$ Cypher A
001011010

5 $\rightarrow$ Homomorphic Encryptor $\rightarrow$ Cypher B
100100110

2xCypher $\rightarrow$ Homomorphic Decryptor $\rightarrow$ 6
0020220202

Homomorphic Encryption for Safe AI
Homomorphic Encryption

3 → Homomorphic Encryptor → Cypher A
   001011010

5 → Homomorphic Encryptor → Cypher B
   100100110

2xCypher → Homomorphic Decryptor → 6
   0020220202

Cypher A + Cypher → Homomorphic Decryptor → 8
   101110210

Homomorphic Encryption for Safe AI
Homomorphic Encryption

- Partially Homomorphic Encryption (PHE)
  - you can only do some operations, such as addition or multiplication

- Somewhat Homomorphic Encryption (SHE)
  - you can do any operation, but only a few times

- Fully Homomorphic Encryption (FHE)
  - unlimited number of any operation
Homomorphic Encryption
Homomorphic Encryption

<table>
<thead>
<tr>
<th>Plain Space</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cypher Space</td>
<td>0</td>
<td>10</td>
<td>20</td>
<td>30</td>
<td>40</td>
<td>50</td>
<td>60</td>
<td>70</td>
<td>80</td>
<td>90</td>
<td>100</td>
</tr>
</tbody>
</table>

**Challenge:** hide a number between 0 and 10 (our “plaintext”)

**Constraints:**
- Somewhere between 0 and 100
- Only we know what it is
- You can add encrypted numbers together
Homomorphic Encryption

Plain Space

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
</table>

Cypher Space

<table>
<thead>
<tr>
<th>0</th>
<th>10</th>
<th>20</th>
<th>30</th>
<th>40</th>
<th>50</th>
<th>60</th>
<th>70</th>
<th>80</th>
<th>90</th>
<th>100</th>
</tr>
</thead>
</table>

\[ P = 2 \]
\[ C = P \]
Homomorphic Encryption

Plain Space

Cypher Space

\[ P = 2 \]

\[ \text{Secret} = 10 \]

\[ C = \text{radient} \cdot \text{secret} + P \]
Homomorphic Encryption

Plain Space

Cypher Space

\[ P = 2 \]
\[ \text{Secret} = 10 \]
\[ C = \text{gradient} \cdot \text{secret} + P \]

\[ \frac{22 + 53}{5} = \frac{75}{5} = 15 \]
\[ 2 + 3 = 5 \]

Homomorphic Encryption for Safe AI
Homomorphism Encryption

Plain Space

Cyphered Space

\[ P = 2 \]
\[ \text{Secret} = 10 \]
\[ C = \text{radient} \cdot \text{secret} + P \]

22 \rightarrow 2
53 \rightarrow 3
2 + 3 = 5
22 + 53 = 75 \rightarrow 5

Homomorphic Encryption for Safe AI
Homomorphic Encryption

With the secret key
Homomorphic Encryption

Cypher Space

Without the secret key

Homomorphic Encryption for Safe AI
Homomorphic Encryption + Federated Learning

Jane's Data
Jack's Data
Joe's Data

AI Inc.

Federated Learning for Safe AI
Homomorphic Encryption + Federated Learning

Jane's Data

Jack's Data

Joe's Data

AI Inc.

INITIAL Model

Federated Learning for Safe AI
Homomorphic Encryption + Federated Learning

AI Inc.

INITIAL Model

Federated Learning for Safe AI
Homomorphic Encryption + Federated Learning

Federated Learning for Safe AI
AI Inc.

Homomorphic Encryption
+ Federated Learning

Jane's Data

Jack's Data

Joe's Data

Federated Learning for Safe AI
Homomorphic Encryption + Federated Learning

Jane's Data

Jack's Data

Joe's Data

Federated Learning for Safe AI
Homomorphic Encryption + Federated Learning

Jane’s Data

Jack’s Data

Joe’s Data

Al Inc.

Federated Learning for Safe AI
Homomorphic Encryption + Federated Learning

Jane's Data

Jack's Data

Joe's Data

Federated Learning for Safe AI
Potential Solution

- **Train A.I.** on data we cannot see without revealing the AI or its training updates to anyone?
  - Homomorphic Encryption
  - Multi-Party Computation
Introduction to Multi-Party Computation for Safe AI
Multi-Party Computation

\[ a = 5 \rightarrow \text{Share Splitter} \rightarrow [1, -3, 5, 0, 2] = \text{shares}_a \]
Multi-Party Computation

For Safe AI

\[\begin{align*}
a &= 5 & \rightarrow & \text{Share Splitter} & \rightarrow & [1, -3, 5, 0, 2] = \text{shares}_a \\
b &= 3 & \rightarrow & \text{Share Splitter} & \rightarrow & [2, -5, 8, -3, 1] = \text{shares}_b
\end{align*}\]
Multi-Party Computation

\[ a = 5 \rightarrow \text{Share Splitter} \rightarrow [1, -3, 5, 0, 2] = \text{shares}_a \]

\[ b = 3 \rightarrow \text{Share Splitter} \rightarrow [2, -5, 8, -3, 1] = \text{shares}_b \]

<table>
<thead>
<tr>
<th>Person 1</th>
<th>Person 2</th>
<th>Person 3</th>
<th>Person 4</th>
<th>Person 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>(s_a = 1)</td>
<td>(s_a = -3)</td>
<td>(s_a = 5)</td>
<td>(s_a = 0)</td>
<td>(s_a = 2)</td>
</tr>
<tr>
<td>(s_b = 2)</td>
<td>(s_b = -5)</td>
<td>(s_b = 8)</td>
<td>(s_b = -3)</td>
<td>(s_b = 1)</td>
</tr>
<tr>
<td>(s_c = 3)</td>
<td>(s_c = -8)</td>
<td>(s_c = 13)</td>
<td>(s_c = -3)</td>
<td>(s_c = 3)</td>
</tr>
</tbody>
</table>

Multi-Party Computation for Safe AI
Multi-Party Computation

\[ a = 5 \rightarrow \text{Share Splitter} \rightarrow [1, -3, 5, 0, 2] = \text{shares}_a \]

\[ b = 3 \rightarrow \text{Share Splitter} \rightarrow [2, -5, 8, -3, 1] = \text{shares}_b \]

<table>
<thead>
<tr>
<th>Person 1</th>
<th>Person 2</th>
<th>Person 3</th>
<th>Person 4</th>
<th>Person 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>s_a = 1</td>
<td>s_a = -3</td>
<td>s_a = 5</td>
<td>s_a = 0</td>
<td>s_a = 2</td>
</tr>
<tr>
<td>s_b = 2</td>
<td>s_b = -5</td>
<td>s_b = 8</td>
<td>s_b = -3</td>
<td>s_b = 1</td>
</tr>
<tr>
<td>s_c = 3</td>
<td>s_c = -8</td>
<td>s_c = 13</td>
<td>s_c = -3</td>
<td>s_c = 3</td>
</tr>
</tbody>
</table>

\[ \text{shares}_c = [3, -8, 13, -3, 3] \rightarrow \text{Share Combiner} \rightarrow 8 \]
Multi-Party Computation+
Federated Learning

Jane's Data

Jack's Data

Joe's Data

Federated Learning for Safe AI
Multi-Party Computation + Federated Learning

Jane's Data
Jack's Data
Joe's Data

AI Inc.
INITIAL Model

Federated Learning for Safe AI
Multi-Party Computation+
Federated Learning

Jane's Data

Jack's Data

Joe's Data

AI Inc.

Jane's Public Share

Model's Public Share

Federated Learning

Multi-Party Computation+
Federated Learning

Federated Learning for Safe AI
Multi-Party Computation+ Federated Learning

AI Inc.

Jane’s Public Share

Jack’s Public Share

Joe’s Public Share

Training Ensues

Federated Learning for Safe AI
Potential Solution

- **Train** A.I. on data we cannot see without revealing the AI or its training updates to anyone?
  - Homomorphic Encryption
  - Multi-Party Computation
Potential Solution

- **Train** AI on data we cannot see without revealing that AI or its training gradients to anyone (FL + HE + MPC)

- **Share** the ownership of a trained AI such that its usefulness is public while its input data, contents, and output predictions are secret - even to the owners of the AI. (MPC)

- **Price** training data we cannot see competitively with other data which we also cannot not see (GT + STAKING + SC + PNP)
Introduction to Gradient Marketplaces for Safe AI
Pricing Unseen Data

Federated Learning for Safe AI
Pricing Unseen Data

Federated Learning for Safe AI
Outline

- **Why**: the AI Business Model has privacy problems
- **How**: an Introduction to the Core Technologies of OpenMined
  - Federated Learning
  - Homomorphic Encryption
  - Multi-Party Computation
  - Gradient Marketplace
- **Roadmap & Demos**
Status Update

- **January Hackathon:** 29 Cities - 400+ online - 70+ In Person
- **Growth Stats:** 2400 Members in Slack - 145 GitHub Committers
- **Recent Milestones:**
  - **PyTorch over Peer-to-Peer** - the foundation of Secure/Private AI
  - **OpenMined Grid** - UK model trained in Canada in 15 secs - Jan 24
  - **Reinforcement Learning** - worked with Unity’s “ML Agents” Team
Project Roadmap

- Federated Learning via PyTorch
- MPC Training via PyTorch
- Rapid Grid Payment via Coinbase
- Private Application Integration
Introduction to Functional Encryption for Safe AI
Functional Encryption

\[ a = [1, 2, 3, 4, 5] \rightarrow \text{Functional Encryptor} \rightarrow \text{cypher}_a \]
Functional Encryption

\[ a = [1, 2, 3, 4, 5] \rightarrow \text{Functional Encryptor} \rightarrow \text{cypher}_a \]

\[ b = [0, 1, 0, 0, 0] \rightarrow \text{Functional Encryptor} \rightarrow \text{cypher}_b \]
Functional Encryption

\[ a = [1, 2, 3, 4, 5] \rightarrow \text{Functional Encryptor} \rightarrow \text{cypher}_a \]

\[ b = [0, 1, 0, 0, 0] \rightarrow \text{Functional Encryptor} \rightarrow \text{cypher}_b \]

\[ \text{cypher}_a \rightarrow \text{Encrypted Dot Product} \rightarrow 2 \]

\[ \text{cypher}_b \rightarrow \text{Encrypted Dot Product} \rightarrow 2 \]