# Final Project Proposal

**Members:**

- Karl Eirich
- Kasha Muzila

**Proposed Work:**

Making purchases online and exchanging money with friends has never been easier with apps like Venmo, Cashapp, Zelle, and PayPal. However, using digital wallets can potentially expose sensitive information such as where they live, what school they go to, their daily schedule, their network of friends, and even illegal or controversial activities. We propose to look into potential privacy issues using Venmo data and how we can mitigate them.

We want to look into specific privacy threats: membership disclosure, identity disclosure, and inference threats. Membership disclosure will expose the content described for the Venmo purchase (i.e., rent payments, therapy payments, school payments, etc.), which can help the attacker identify the victim within the dataset and determine their schedule. Identity disclosure will expose the victim's location and whom they are friends with, making them vulnerable to an attack. Lastly, inference threats such as the victim's purchases of drugs and alcohol or emojis that profile them can benefit an attacker. However, we would like to focus primarily on membership and identity disclosures for this proposal.

Before writing this proposal, we analyzed the Venmo data and tried to trace it back to sensitive information, in which we succeeded. The information exposed was either membership disclosure, identity disclosure, or inference threats, as previously described.

For our proposal, we would like to use the Venmo database, Python, and Jupyter Notebooks to visualize how substantial these threats may be and use SWOT (strength, weakness, opportunity, threat) mitigation techniques to improve Venmo's privacy settings for their users.

**Survey of Related Work:**

- Dataset
  - venmo-data
- Previous W233 project
  - Breaking Venmo's Privacy
  - [Blog] Venmo's Information Disclosure
- Mentioned by previous W233 project
  - Public By Default

**Preliminary Results (Optional):**

- None

**Potential Contributions:**

- Karl will handle data ingestion and processing
- Kasha will develop privacy threat insights and visualizations

**Proposed Milestones:**

- Week 1
  - Write data ingestion script and begin processing code
- Week 2
  - Finish processing code and start developing insights
- Week 3
  - Start visualizing insights and crafting narrative
- Week 4
  - Identify and analyze mitigation suggestions
- Week 5
  - Finish developing insights and start writing paper
- Week 6
  - Start creating slide deck
- Week 7
  - Finish writing paper and creating slide deck
- Week 8
  - Finalize and present project

Below is an apporoximate Gannt Chart of our schedule and milestones:

| | Week 1 | Week 2 | Week 3 | Week 4 | Week 5 | Week 6 | Week 7 | Week 8 |
|---|---|---|---|---|---|---|---|---|
| **Data Ingestion script and processing code** | | | | | | | | |
| **Insights** | | | | | | | | |
| **Crafting narrative** | | | | | | | | |
| **Mitigation suggestions** | | | | | | | | |
| **Writing paper** | | | | | | | | |
| **Creating slide deck** | | | | | | | | |
| **Finalize and present project** | | | | | | | | |