

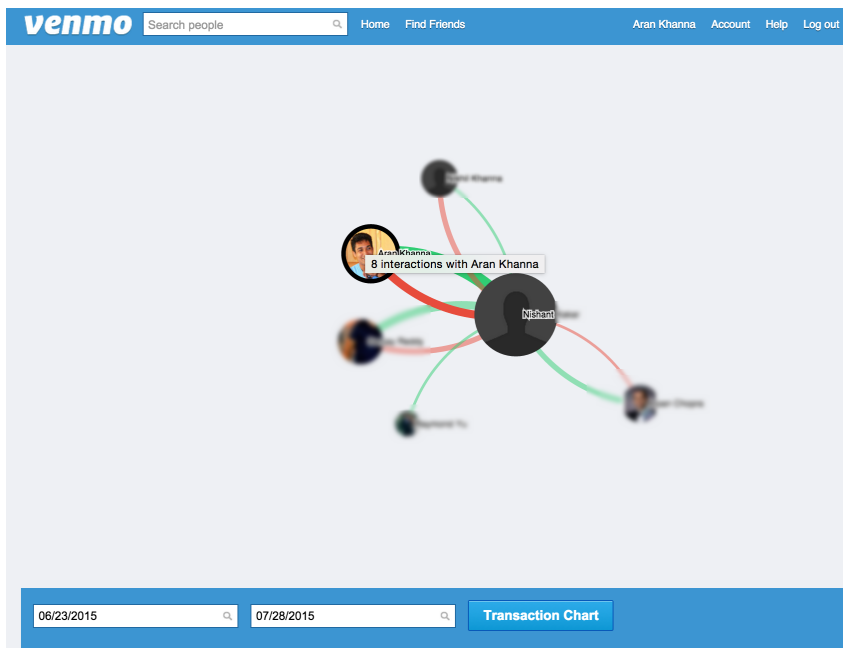


Venmo'ed: Sharing Your Payment Data With the World

Aran Khanna

Highlights

- The Venmo app allows people to pay each other online. I created an extension that visualizes information Venmo makes publicly available
- I analyzed the transactions of 350,000 Venmo users and found that 74% had at least 5 public transactions, with 21% averaging a public transaction more than once a week
- My extension can identify relationships between users, including how much time they spend together. It can also identify members of private social organizations, attendees of private events, and even users' food purchases



Demo screenshot of visualization created by the Money Trail Extension of transactions between the central user, Nishant, and his friends on Venmo.

Abstract

The app Venmo has quickly become one of the most popular mobile, peer-to-peer payment platforms among Millennials in the United States. The app allows users to pay each other and share the payment message, recipient and time with other users of the app. In the past Venmo has had its share of security and privacy issues and has even been the target of regulatory action [12]. Despite this, Venmo has continued to have features and designs that publicly reveal large amounts of user data. In addition to the privacy implications of revealing user data, previous papers have shown that this information can be used in social engineering attacks to defraud users [10]. I hypothesized that Venmo's payment sharing feature, which defaults to sharing all transactions publicly with any user of the app, causes users to leak sensitive personal data about themselves, and that the problem is widespread.

Results summary: I created a Chrome extension to analyze the extent of the information Venmo was publicly sharing about its users. I found that many users were revealing potentially sensitive data about their social lives and purchasing habits through their use of the app. Furthermore, I analyzed the transactions of 350,000 users to uncover that the 74% of users on the site were sharing at least 5 public transactions, and 21% were sharing more than once a week, meaning that a significant number of users have enough shared data on the site to be potentially vulnerable to the kind of analysis I demonstrate with the extension. With this paper I am publishing the extension I created, so that users of the site can discover for themselves how much data is being shared and what can be learned.

Introduction

How private are your credit card purchases? Generally, neither you nor the recipient of your payment would publicly broadcast a transaction. In a 2014 survey, 87% of Americans considered credit card data to be moderately or extremely private [1]. That does not mean data about credit card transactions are not shared. While friends or other curious third parties can't directly access this data, credit card companies share transaction information for authentication, marketing, and other purposes. The credit card companies, under the Gramm-Leach-Bliley Act, must protect certain aspects of your identity by removing personally identifiable information, such as your card number, from the data, and notifying you of the third parties with whom they are sharing your data [2].

What about new kinds of payment instruments? Bitcoin publishes the details of your transaction as tied to a Bitcoin ID, though that transaction can only be associated with you if the Bitcoin ID is tied to your identity [3]. Paypal is in many ways similar to card purchases. While Paypal can analyze your transaction data and share it with affiliates and trusted third parties (including for legal services, billing, and fraud prevention

services) as outlined by their privacy policy, the company may only share information with additional parties if given your “consent or direction” [4].

Increasingly people, particularly Millennials, are using Venmo, the social, peer-to-peer payment app that launched publicly in 2012 [5]. In September 2013 PayPal acquired Venmo's parent company, Braintree, making Venmo a member of the Paypal corporate family [6]. Venmo has since grown significantly, processing \$2.4 billion in transactions in 2014 [7]. Users can conduct transactions via Venmo on iOS and Android devices, and on the web app at Venmo.com.

How private are Venmo transactions?

The default setting for transactions on Venmo is to publicly share online (1) the names of the payer and the recipient, usually taken from linked Twitter or Facebook accounts, (2) the date of the transaction, and (3) the message written by the user that initiated the transaction, which may give enough information to infer what the payment is for (Figure 1a) [8]. Since payments on Venmo are frequently reimbursements to split costs for a shared purchase, examining a user's public transaction data feed provides insight into the financial life and network of a user over time. Venmo's privacy settings do offer users other options besides publicly sharing their transaction data (Figure 1b). According to my understanding of Venmo's description of these privacy settings in their help center [9], the visibility of each transaction depends on a complicated decision tree of at least 16 scenarios, as shown in Figure 1c. Visibility is determined by the settings of the user (the transaction initiator or the respondent) who has chosen the more restrictive privacy setting for that specific scenario.

1. User A initiates the transaction by sending a Pay or Charge request to User B.
2. If User B sets their “Can share transactions involving me” setting to Everyone, then the transaction is visible to the Public, Friends (connected on Venmo), or Private (only the participants in the transaction) depending on User A's “Default audiences for future transactions” setting.
3. If User B sets their “Can share transactions involving me” setting to Only Me, then the transaction is only visible to the participants involved regardless of User A's “Default audiences for future transactions” setting.

Under Venmo's complicated privacy decision tree, a user needs to remember to change two similar-sounding settings to the most private option in order to guarantee that by default all future transactions, regardless of who initiates the transaction, are only visible to the participants involved.

1. If a user sets their “Default audiences for future transactions” setting as Private but leaves their “Can share transactions involving me” setting as Everyone,

- then all transactions they initiate will be private, but all future Pay or Charge requests that they respond to will have the audience determined by the requester's "Default audiences for future transactions" setting. These transactions might even be Public if the requester did not change their privacy setting away from the default option.
2. If a user sets their "Default audiences for future transactions" setting as Public but their "Can share transactions involving me" setting as Only Me, then all transactions they initiate are public, but all future Pay or Charge requests that they respond to will be private and only visible to the participants.

According to a 2014 paper, as many as 50% of transactions on Venmo are publicly shared [10].

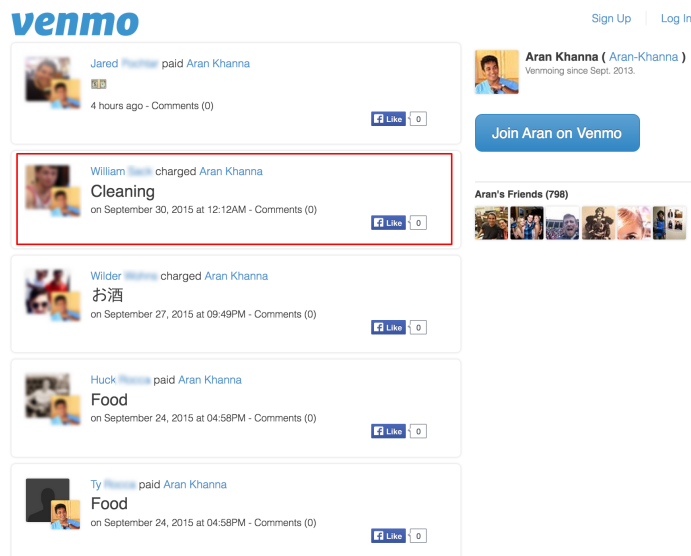


Figure 1a. A screenshot of my public feed on 10/15/15, which any user who navigates to my Venmo page while not logged into the site will see. It contains the most recent 5 public transactions involving me. A charge from my roommate on 9/30/15 for "Cleaning" is highlighted with the red box.

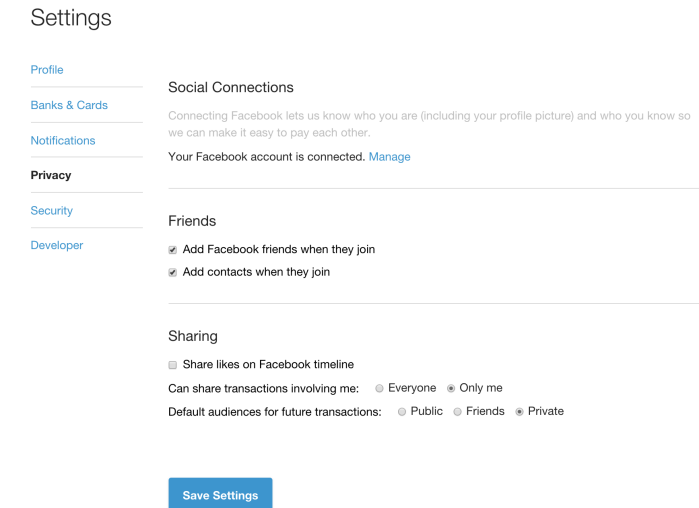


Figure 1b. Screenshot of my privacy settings on the Venmo.com web app. This screenshot was taken on 9/5/15. I had specified that by default all transactions involving me will be private regardless of who initiates the transaction. I set the “Can share transactions involving me” setting to Only Me and set the “Default audiences for future transactions” setting to Private.

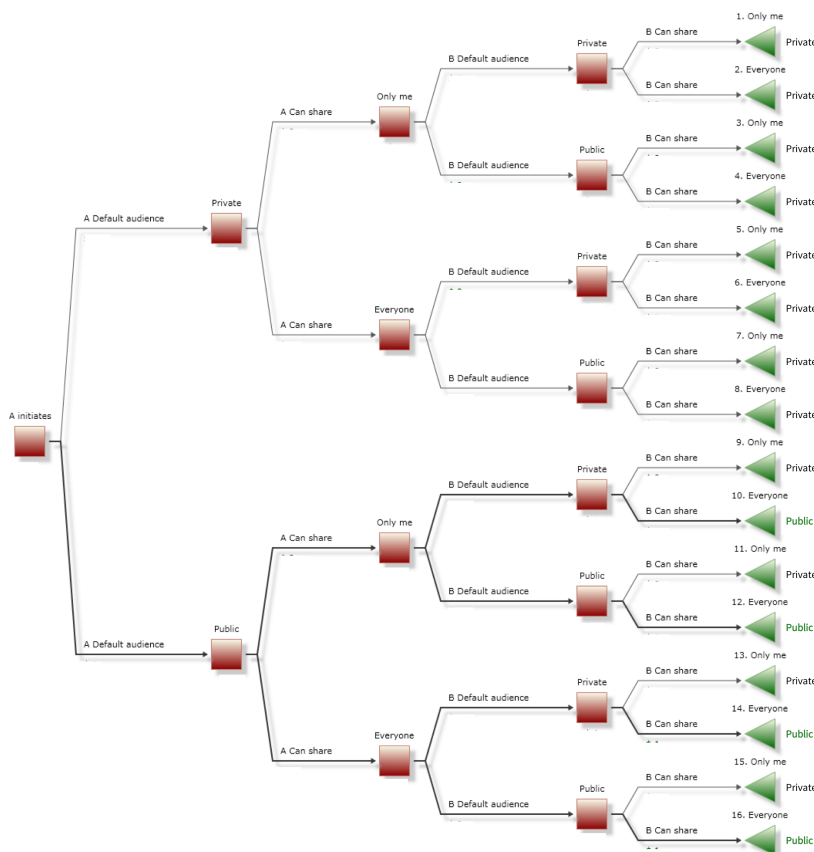


Figure 1c. The simplified Venmo decision tree determining the visibility of a transaction according to the privacy settings of the initiator and the recipient of the transaction. “Default audience” indicates the “Default audiences for future transactions” setting and “Can share” indicates the “Can share transactions involving me” setting. This decision tree assumes that pay and charge requests are treated the same and examines the extremes of each setting without looking at the Friends Only option for “Default audiences for future transactions.” I tested the 16 possible scenarios with a user on Venmo’s Android app version 6.18.1 (User A) initiating transactions with a user on Venmo’s iOS app version 6.15.4 (User B). Transactions are by default Public in 4 different scenarios.

Venmo’s privacy settings changed in 2015, as seen on Android in Figure 2. A new version of the app added a “Transactions Involving You” setting that is the same as the “Can share transactions involving me” setting on the Venmo website. However, the change log did not notify users about the new setting when it was added to the app [11]. Furthermore, as of version 6.18.1 the only way on Android to make all previously shared transactions private is time-consuming, requiring manually setting each individual past transaction to Private.

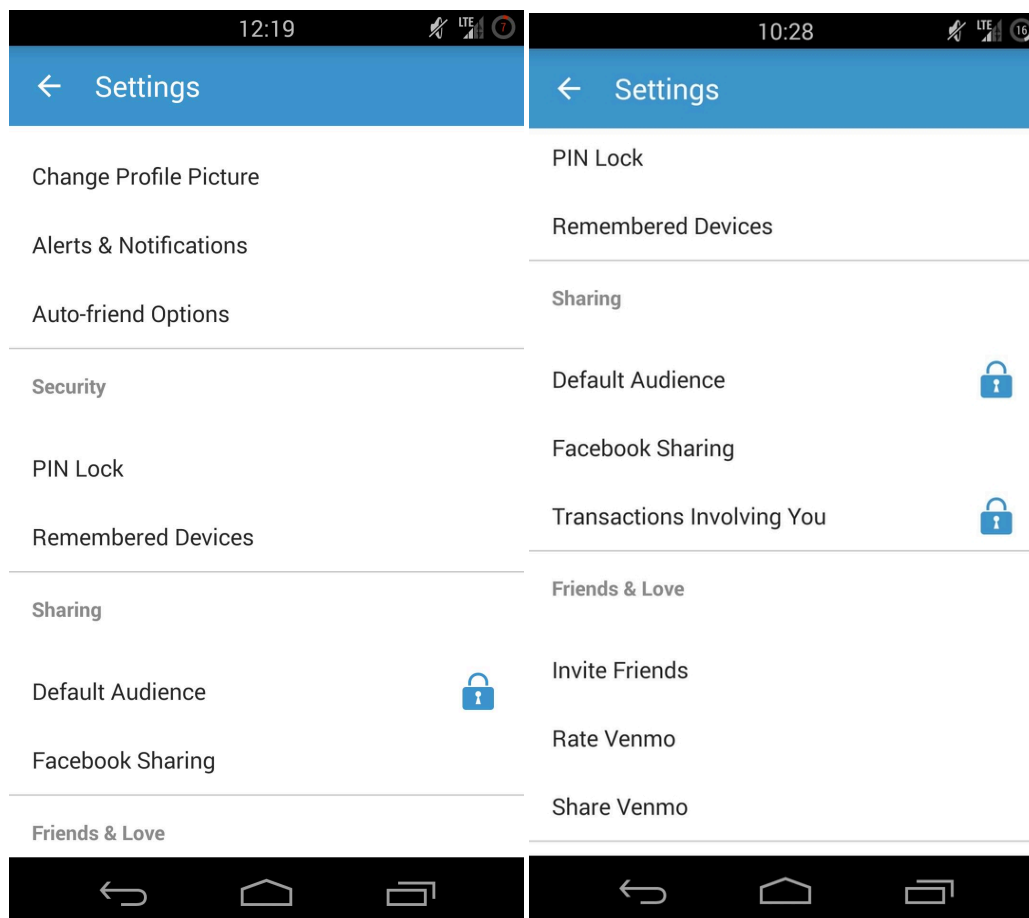


Figure 2. Screenshots of the privacy settings on the Android version of Venmo, before (left) and after (right) an update to version 6.18.1. The update added the ability to make all transaction payments sent to the user private through the “Transactions Involving You” setting.

Background

Researchers have criticized Venmo for loose security practices that could compromise user accounts as well as data, particularly in the May 2014 paper "Security Research of a Social Payments App" by Kraft et al [10]. The paper highlighted a series of issues, including the possibility of a brute-force attack against the SMS payment authorization system (which could allow attackers to execute payments to themselves from hacked user accounts), and the possibility that any user on the network could view all transactions shared by a user with only their friends via an unofficial API. The paper also highlighted how the ability to change your Venmo user name at will, the lack of a UI differentiation between charges from friends vs. charges from strangers, and the visibility of payment patterns in past public transactions, lead to the possibility of sophisticated social-engineering attacks on the platform.

After the disclosure of these findings, according to the paper, Venmo made the SMS payment authorization system more secure and removed the unofficial API call that publicly leaked payments shared with friends only. However, there was no specific fix for the transaction-sharing features and design issues that facilitated social-engineering attacks. Venmo's official response to this concern was: "we are constantly improving how we mitigate risks around social engineering and identity fraud. We currently minimize these risks by using various rate limits, transaction caps, and internal monitoring tools to detect and eliminate abuse" [10].

Beyond pressure from academics to tighten security, Venmo's security and privacy policies were the subjects of regulatory intervention by the State of California's Department of Business Oversight in July of 2014 [12]. In addition to addressing 19 other issues, the regulatory notice mandated that Venmo establish procedures for dealing with fraud loss and consumer privacy within 60 days. Although Venmo complied with the regulatory notice in 2014, the company received public criticism on *Slate* in February 2015 for its lack of adequate fraud detection/alerting mechanisms and for the absence of basic security features like two-factor authentication. The *Slate* writer showed how these failures could lead to the loss of thousands of dollars from users with hacked accounts [13]. Venmo responded by adding two-factor authentication for all users by default [14]. On September 15, 2015, *Slate* again reported that Venmo users were vulnerable to fraudulent charges and quoted users who were unsatisfied with Venmo's response to their experiences with fraud [15].

Beyond security, researchers and others have also raised and demonstrated their concerns about the privacy implications of the sharing features in Venmo. For example, Vicemo is an app created by Mike Lacher and Chris Baker that pulls from Venmo's public feed API, returning a set of the most recent public transactions from all users and displaying any transactions whose messages contain references to sex, booze, or drugs [16]. After Vicemo's release in February 2015, *The Washington Post*, *Business Insider* and other publications ran stories questioning the privacy issues raised by publicly sharing payments [17, 18]. Venmo responded in a February 2015 blog post listing their safety and security measures but failed to address any of the questions about privacy issues raised by the sharing of transactions [19]. As of October 2015, Vicemo is still up and running.

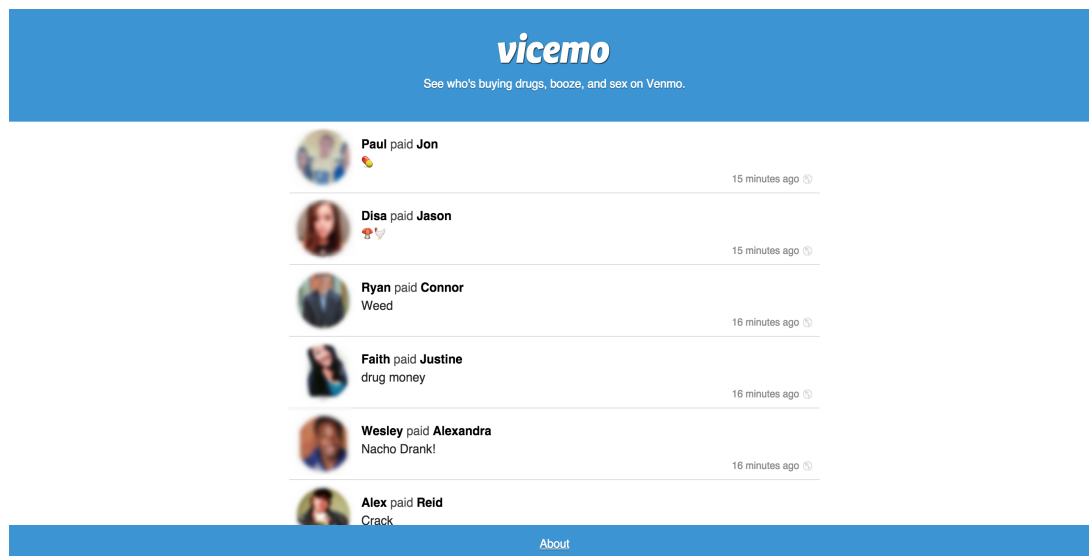


Figure 3. A screenshot of Vicemo displaying transactions it had scraped in the past 20 minutes. Any public Venmo transaction with a message that contains words or emoji associated with drugs, sex, or alcohol is displayed [16].

Methods

Given the large percentage of transactions that are shared publicly on Venmo, coupled with the possibly sensitive nature of the messages accompanying these transactions, I theorized that a significant fraction of users were sharing Venmo activity that could be analyzed to reveal their potentially private spending patterns as well as accurately model their social graphs. To test this I built a visualization tool, in the form of an extension for the popular Chrome web browser, to highlight and explore the extent of these potential vulnerabilities. Then, to estimate the fraction of users who could fall victim to these vulnerabilities, I scanned hundreds of thousands

of public Venmo profiles to discern the rate at which users are revealing information about their transactions.

My Chrome extension visualizes a user's public Venmo data from their newsfeed page. This approach allowed me to dynamically look through a user's public history and easily see patterns in their interactions with others that could be used to infer personal information. This extension also has the benefit of being easy to distribute, so Venmo users can leverage it to obtain transparent feedback about what sort of data they and those they know are revealing via the app.

My next step was to create code to pull more than 350,000 public Venmo user pages. I then parsed this HTML data to estimate how many public transactions users are exposing over time. This approach, while an estimate and not ideal, allowed me to get a sense of how many users are engaging in public transactions frequently enough to be exposing a significant amount of personal information via the app.

The Extension

The extension is a lightweight program (called a "script") that runs on Google Chrome. After a user logs into Venmo.com and navigates to any Venmo user's newsfeed page, the script runs in the background to detect the source of the historical transaction data populating the newsfeed. It then requests a copy of that historical transaction data and loads it into the visualizations. It is important to note that all data retrieved is normally accessible in the public newsfeed.

Because you must be logged into Venmo to load historical transactions for a user (beyond the five most recent ones), this extension will only work if you have an account on the site. However, once you are logged into the site, you don't have to be connected as a "friend" to an individual on Venmo to view their public data, including transactions, meaning that this extension will work on the newsfeeds of all Venmo users.

The extension does nothing illegal or malicious; rather, it accesses and creates data visualizations on top of data already available to a user through Venmo's user newsfeeds. A full technical overview of the system can be seen in Figure 4. Figures 5 and 6 show examples of the visualizations created with the extension.

I uploaded the extension to the Chrome Web Store, marking it as unlisted. The title of the extension on the Chrome Web Store is "Money Trail" [20], and an open source copy of the extension's code is available in a MIT-licensed Github repository with the title "money-trail" [21]. This repository contains the code and setup instructions for creating the extension from source.

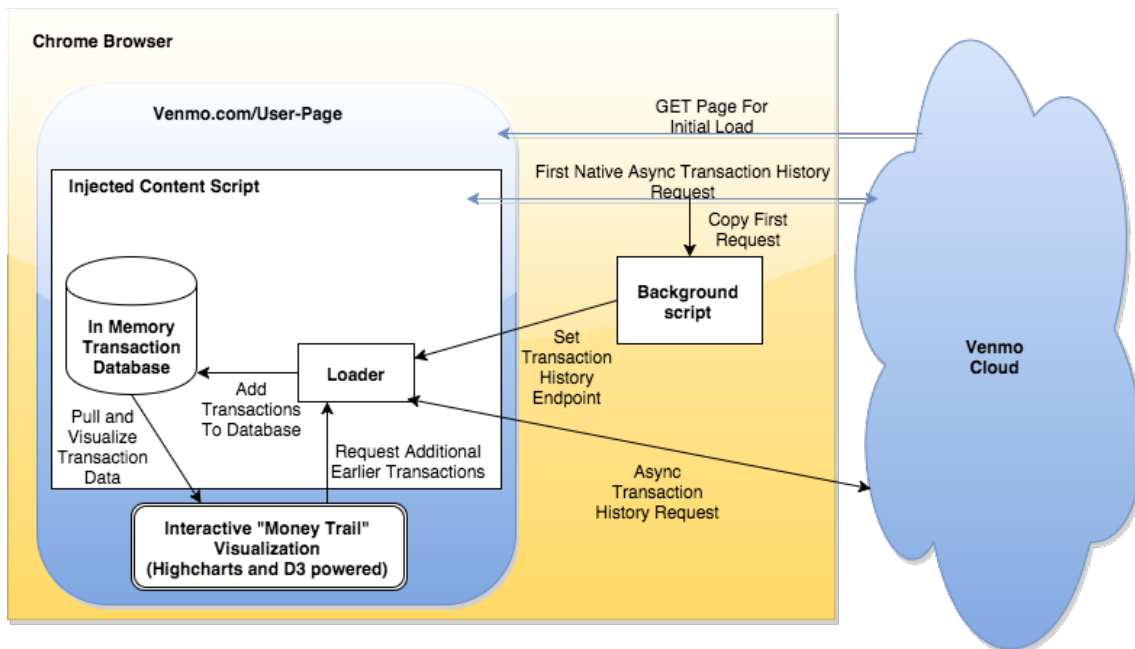


Figure 4. A graphical depiction giving a full technical overview of the Money Trail Chrome extension. White boxes represent the components injected by the extension. The extension consists of a Chrome background script that listens for an asynchronous call from Venmo.com to the unique cloud endpoint that returns a specific user's transaction history. It then passes this endpoint URL to an injected content script running on a Venmo user's newsfeed page. The content script then configures a loader to pull transaction data from that endpoint in the same manner as the native website and load that data into an in-memory database. The content script next injects the visualization control panel into the page and renders a D3-powered bubble graph from the initial set of transactions loaded into the database. If the visualization is switched, a Highcharts-powered chart is rendered from the existing data in the database. If the earliest date in the range is set to before the earliest transaction in the database, the loader is called to pull data from the cloud endpoint until all the transactions in the date range are loaded or there are no more transactions left in the user's history.

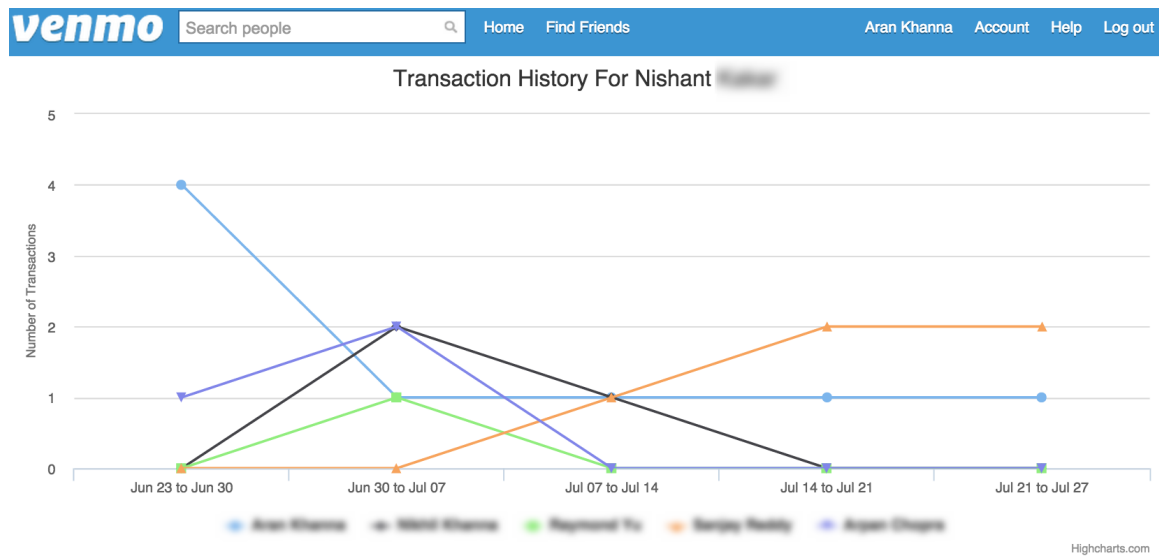


Figure 5a. A screenshot of the Highcharts-powered transaction chart visualization created by the Money Trail extension. The Y axis shows the total number of transactions within a time period on the X axis of the current user with a friend on Venmo. Each colored line indicates transactions with a specific friend.

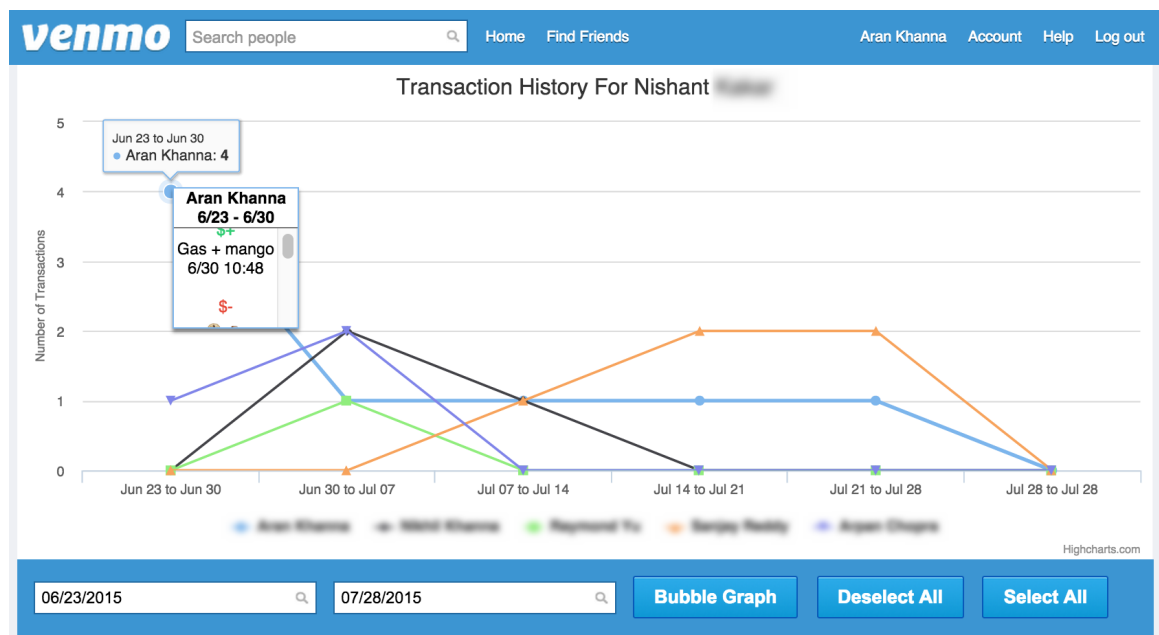


Figure 5b. A screenshot of the pop-up box opened by clicking a data point on the chart. The pop-up lists the specific transactions with that friend over the period on the X axis, as well as the exact times (to the minute) at which funds were sent.

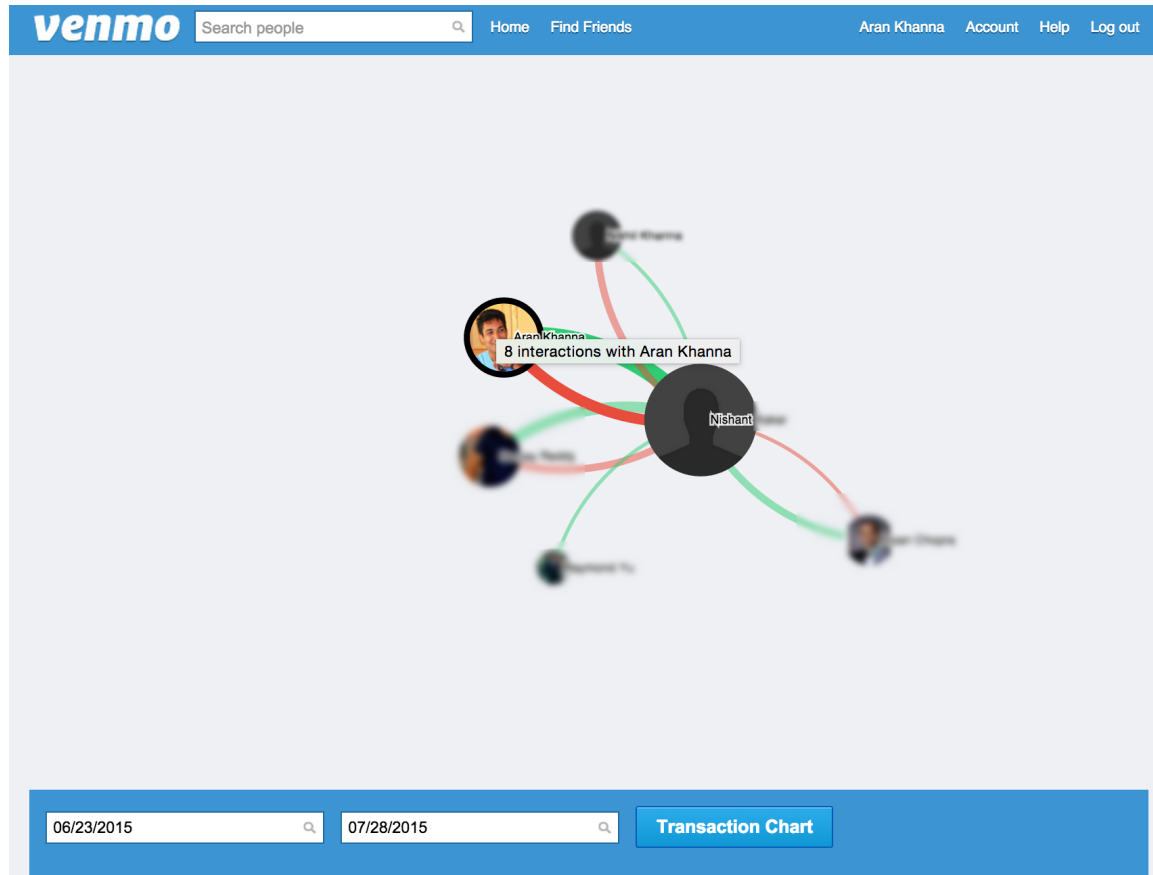


Figure 6. A screenshot of the D3-powered bubble graph visualization created by the Money Trail extension. The size of a non-central user's bubble is proportional to the number of transactions between that user and the central user. The thickness of the red line connecting a non-central user to the central user corresponds to the number of payments sent from the central user to that non-central user, and the thickness of the green line corresponds to the number of payments sent to the central user from the non-central user.

Analysis with the Extension

To perform analysis with the extension, I looked through a series of Venmo profiles of users from whom I was one degree removed on the network (i.e., we were not friends but shared mutual friends) as my initial sample. Since we weren't direct friends, I could only view the public data exposed by these users via the app (semi-public payments sent from mutual friends were also visible). Furthermore, my initial sample consisted of mostly Millennials, who are 18 to 35 and many of whom are still in college. This is representative of the most prominent and fastest growing demographic of Venmo users [22]. After using the extension to analyze the data exposed by these

second-degree connections, I searched for usage patterns among these users that allowed potentially private data to be inferred from corresponding public transactions.

The Scrape and Analysis

To scrape Venmo users' public profiles for data I created a lightweight Python script, publicly available for this study under an MIT License, which performs a breadth-first search through Venmo's network, starting with a seed user, to identify a large sample of users. The script gathers user data by making unauthenticated requests via urllib2 to Venmo users' profile pages, retrieving the public version of the page HTML containing up to 5 of the user's most recent publicly visible transactions. The script saves the HTML of all the user profiles it crawls and parses them to extract how many transactions are going to and from the user as well as how many days ago each of the transactions took place. Additionally, the script generates new user profiles to add to the crawl queue for the breadth first search by scraping the links to other users' profiles from the transaction participants in the current user's feed and then up to 6 additional friends in the current user's abbreviated friends list. These two sets of profile links often have few intersections, so for each user there is a branching factor of up to 11 new links to crawl. Figure 2 shows that running the script on my own public Venmo profile page would have resulted in capturing the 5 public transaction details, the names of the 5 friends who paid or charged me in those transactions, and the names of the 6 friends whose pictures are shown under "Aran's Friends."

I created a dataset for analysis by running the breadth-first search script four times with four different seed profile sets of users who shared no mutual friends. I generated the seed profiles by drawing from clusters of users, not directly connected, who are part of my extended network on Venmo. Each breadth-first crawl was started on September 5, 2015. In total the crawls ran for 3 days, terminating when they ran out of new profiles in the queue or reached 100,000 profiles. After completing the crawls, I de-duplicated and merged the data sets from the separate crawls, yielding 357,177 unique profiles. The dataset of aggregated statistics as well as the raw HTML pages I extracted these statistics from are available publicly with this study [23]. Because Venmo does not publicly release its number of users, there is no way to know for sure what fraction of the user base this represents; however, in 2012 Venmo reportedly had approximately 1.5 million users accounts and \$250 million in payments [10]. In Q2 of 2015, it was reported that Venmo processed over \$1.6 billion in payments [23]. Assuming users grew at the same rate as payments, I estimate that the scrape may reasonably represent somewhere in the range of 3-4% of the network of an estimated 9.6 million users.

I analyzed the dataset to estimate the average time interval between public transactions for most users alongside other metrics. The iPython Notebook used for the analysis is available publicly with this study [23].

Results

Results of Analysis Using the Extension

With the Money Trail extension, I uncovered many usage patterns of the Venmo application that leaked potentially sensitive user data. The first thing I discovered was that many highly active users who publicly shared transactions on the Venmo once a week or more had many transactions related to splitting meals, drinks, etc. with others. The extension allowed me to see with whom the user shared these experiences and when they took place, providing insight into the social life of the user as seen in Figure 7.

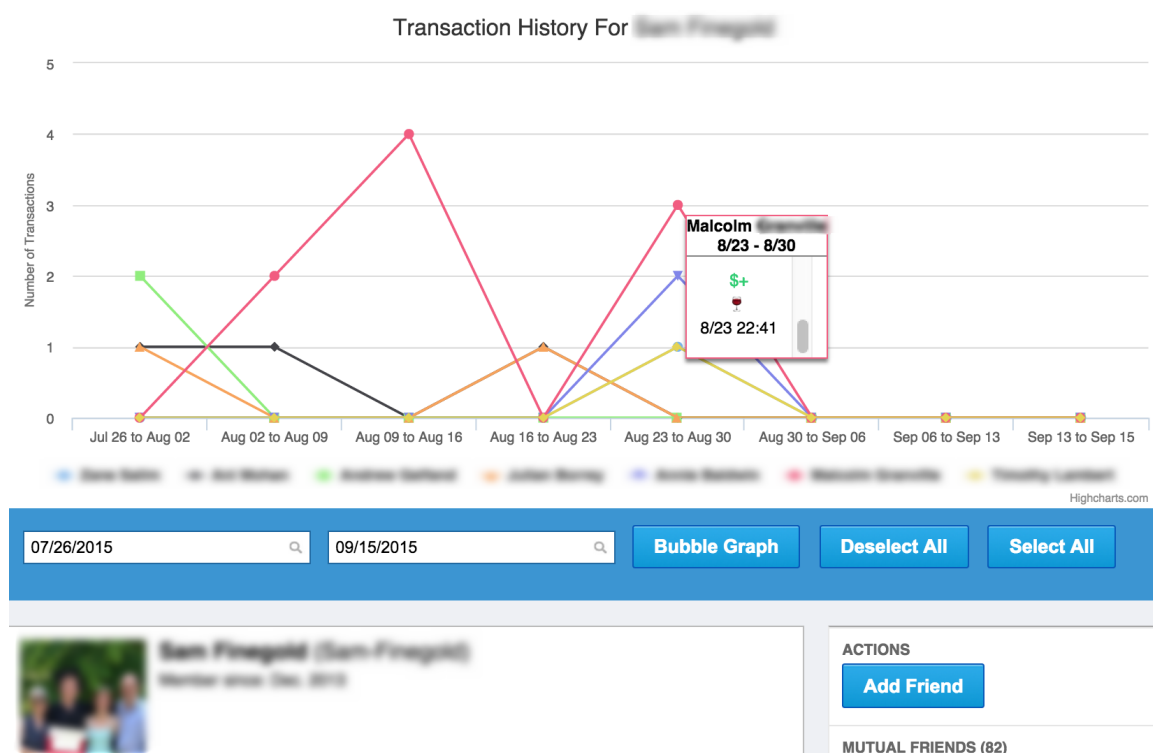


Figure 7. A transaction chart for a user highlighting one of his many recurrent transactions with Malcolm. The wineglass emoji in the message is presumably denoting a payment for drinks they shared on the night of the 23rd, which would be in line with his pattern of transactions with Malcolm for multiple weekly dinners and drinks.

I also found a similar pattern with people splitting Ubers/cabs and even cover charges, giving an even higher-resolution picture of with whom these users interacted the most in their lives. This sort of information seems to correspond well to the social connectedness of users inferred by the bubble graph visualization of their data in Figure 8.

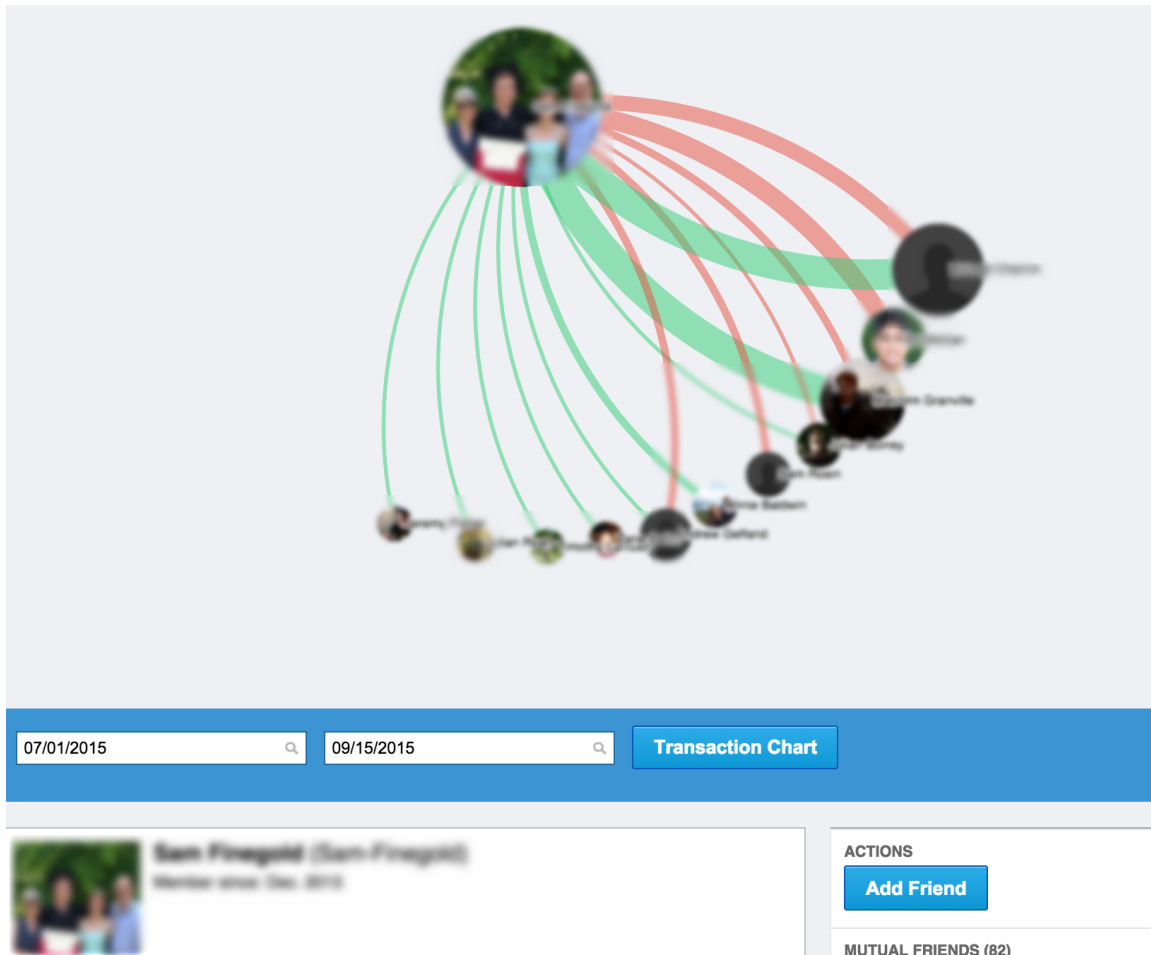


Figure 8. The bubble graph for the user in Figure 7, showing the people with whom he had the most transactions, and hence spent the most time with. His friend Malcolm is the largest of the 3 bubbles, corresponding well with the chart data chart showing them spending a lot of time drinking and eating together.

Repeated patterns in the transaction histories of these relatively frequent Venmo users, such as weekly brunches or meet-ups, were easy to pick out, giving me the power to predict when (and sometimes where) two or more users will spend time together.

I also found that the nature of relationships between users, such as whether two users are roommates, dating, classmates etc., can be readily inferred from the timing, frequency and message context of payments as seen in Figure 9.

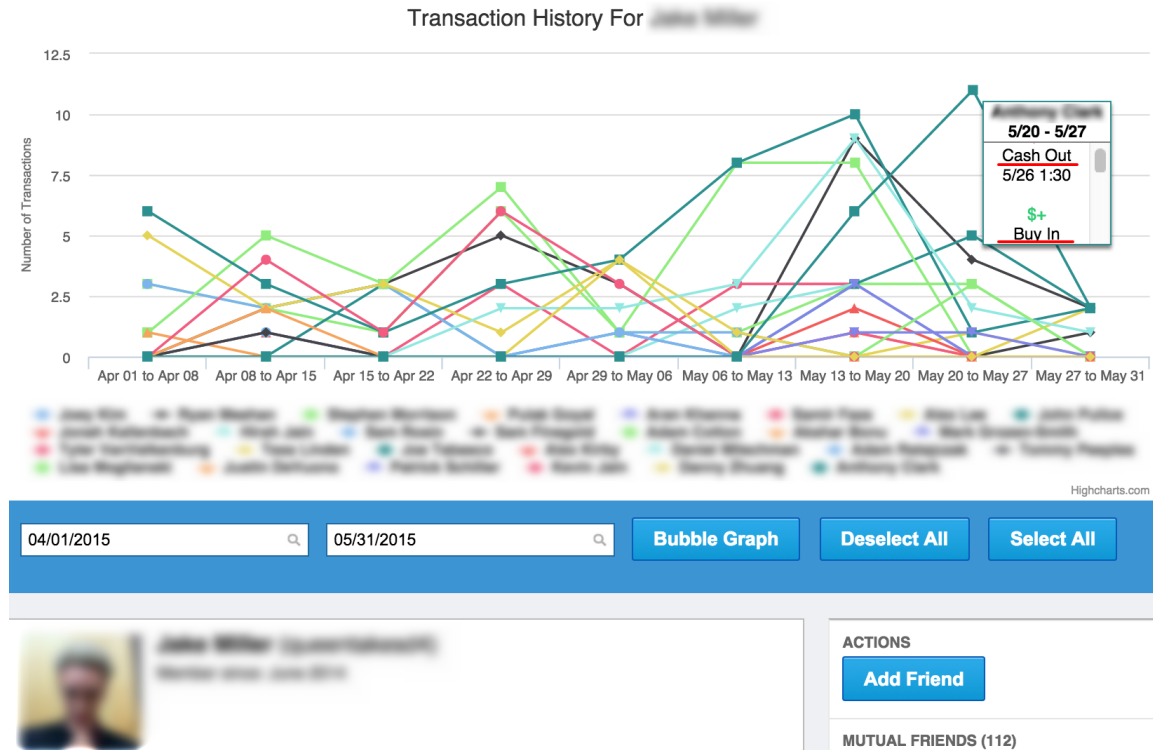


Figure 10. The transaction chart for a user who frequently organizes poker games for a group of friends and collects buy-ins as well as dispenses cash payouts to winners using Venmo. A user is highlighted who bought into a game on 5/26 and subsequently cashed out that that night (signaling he didn't lose all of his buy-in and likely won money in the game).

I also found that many organizations, particularly student organizations on college campuses, create official Venmo profiles that they use to accept payments for things such as merchandise, event tickets, and even membership dues. As seen in Figure 11, this allowed me track annual membership for groups, including several unofficial student organizations.

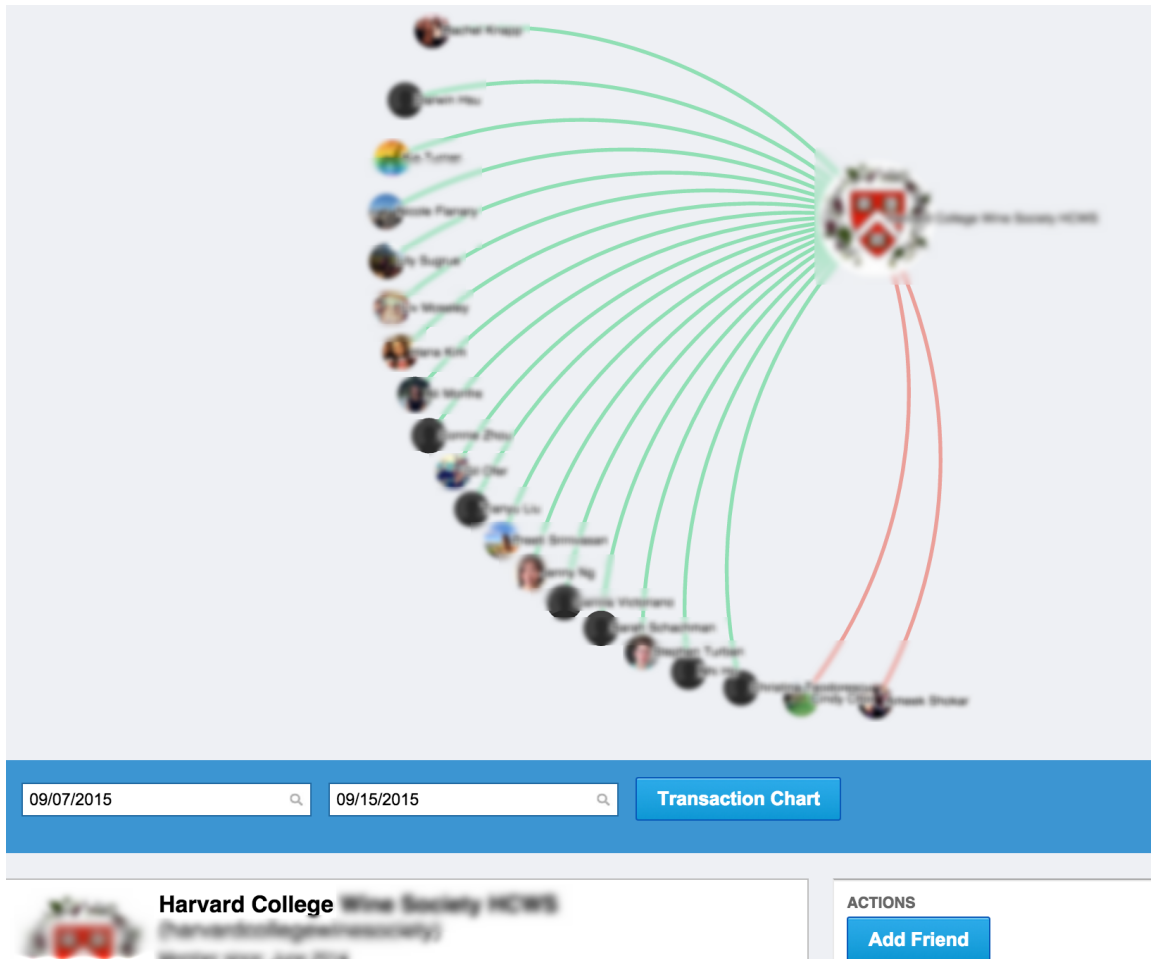


Figure 11. The transaction bubble graph for a certain student-run Harvard College society for the week when the society collected membership dues. Each user connected with a single green line is presumably a member, as they paid dues over this week. The users with red lines going to their bubbles are organizers, presumably being reimbursed for expenses they incurred.

Figure 12 shows that this usage behavior also allowed me to track who purchased what goods and services from various organizations.

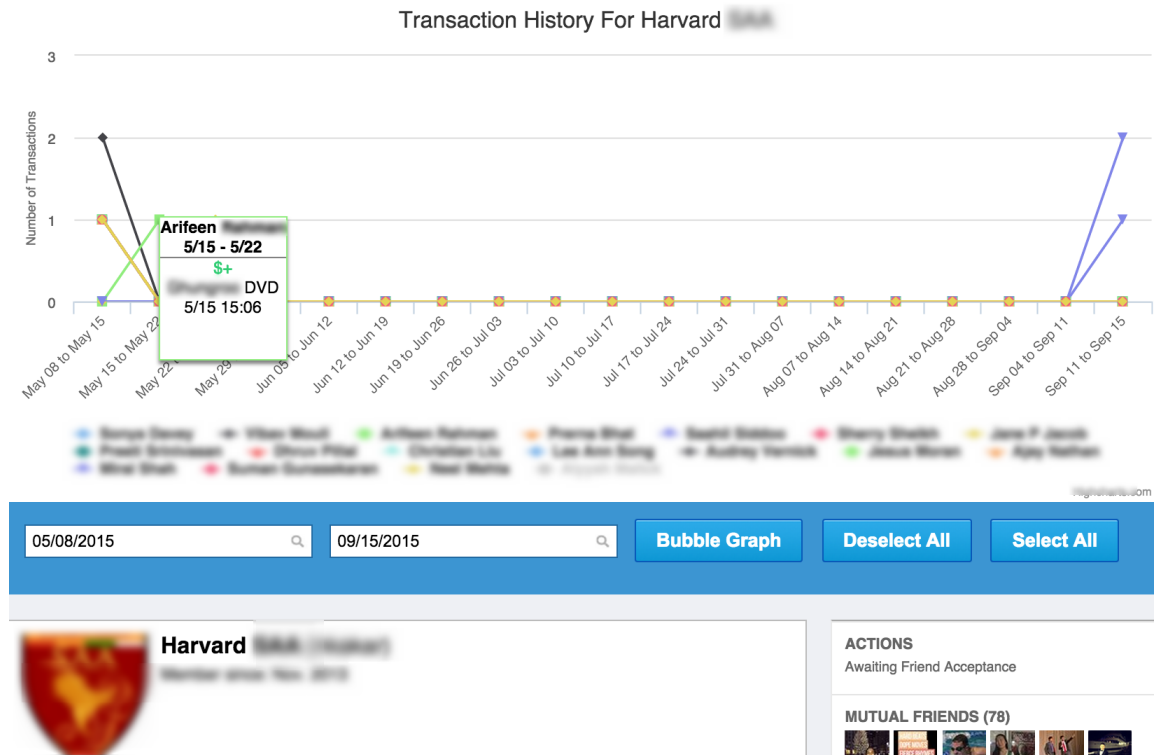


Figure 12. The transaction chart for a student-run Harvard College cultural organization, highlighting that the DVD of an annual show the organization puts on was sold to Arifeen via Venmo on 5/21.

Finally, this behavior allowed me to track attendance at certain organization events where tickets were being sold over Venmo as seen in Figure 13.

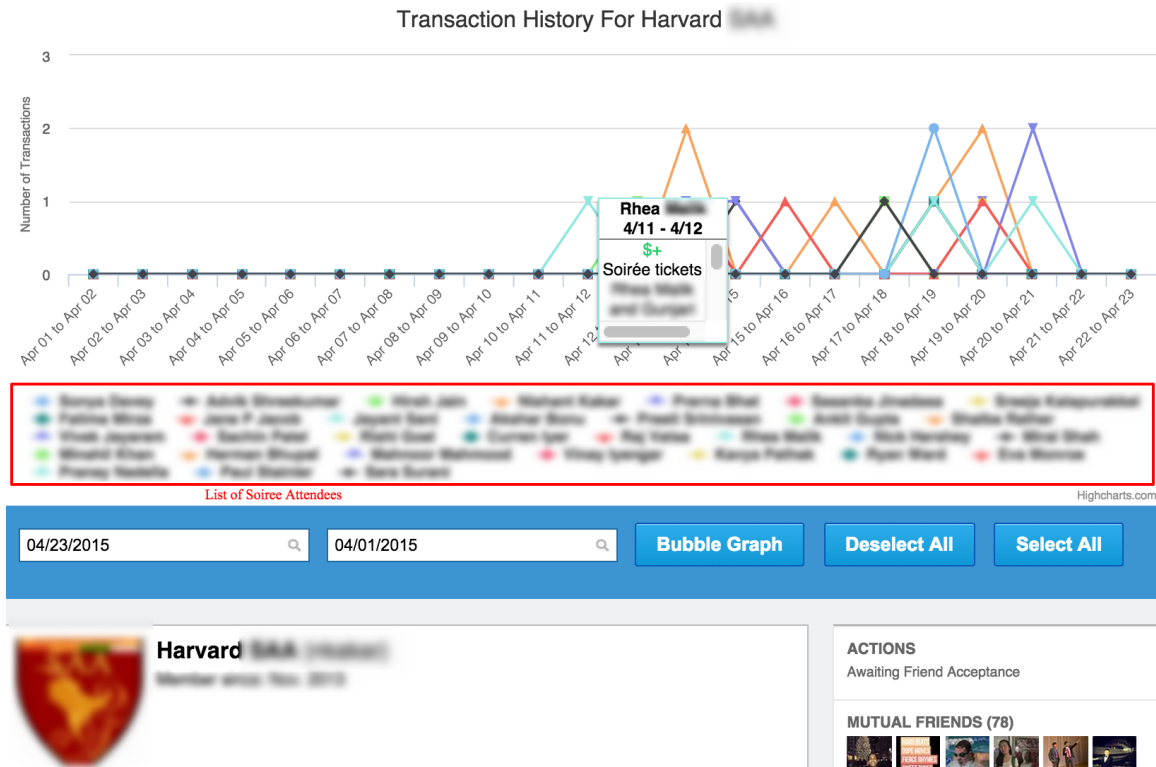


Figure 13. The transaction chart for the same organization shown in Figure 12 over the period from 4/12 to 4/22 when they sold tickets to an event called Soirée. The popup box has an example of one of the transactions of someone paying for a ticket to the event. These transactions allowed me to generate a list of attendees of the event, highlighted in red below the chart.

The last non-standard use case I discovered involved student-run stores on campus that accepted Venmo as a valid payment method. Figure 14 shows the data for a student-operated campus grill at Harvard College that accepts Venmo as a payment for meals. In this data I can see users' specific orders and what times they are getting food, allowing me to predict recurring patterns such as a user's meal time and their usual order.

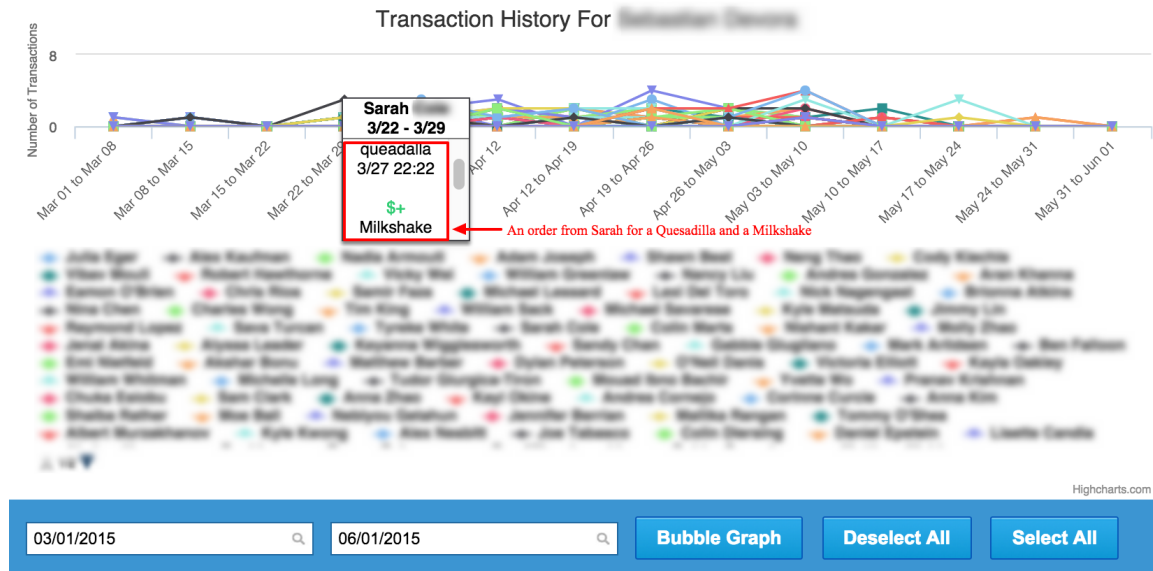


Figure 14. The transaction chart for a campus grill at Harvard College that accepts Venmo. Highlighted is one of the many payments from a student to the grill containing the items ordered.

The Scrape and Analysis

After crawling 400,000 profiles in the breadth-first search script, I de-duplicated the entries, finding that at most I re-crawled 42,892 of the profiles. This means that there was a not-insignificant overlap in the subsets of the social graph crawled by the various scripts, so that bias due to network effects may be an issue. Given more time, a re-crawl from more carefully chosen seed values may be a good way to create a more uniform subset of the graph.

Of the 357,177 unique public profiles I crawled, the vast majority (74%) had 5 transactions visible on their public page (Figure 15). These are potentially heavy users of the service with privacy settings that publicly reveal their transactions.

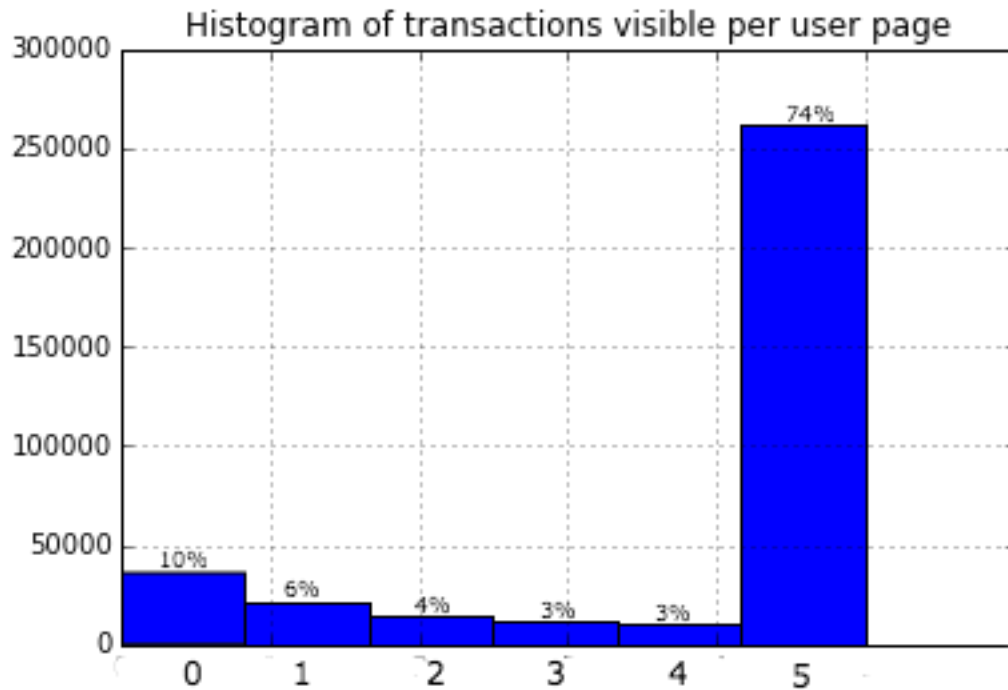


Figure 15. A histogram of the number of transactions publicly exposed on Venmo users public profile pages. The portion in the column labeled 5 have shared 5 or more public transactions.

Diving into this segment of users with 5 shared publicly transactions, I looked at the frequency with which the 5 most recent public transactions on the page occurred and calculated the average wait for the next public transaction from the user. Results are shown in Figure 16.

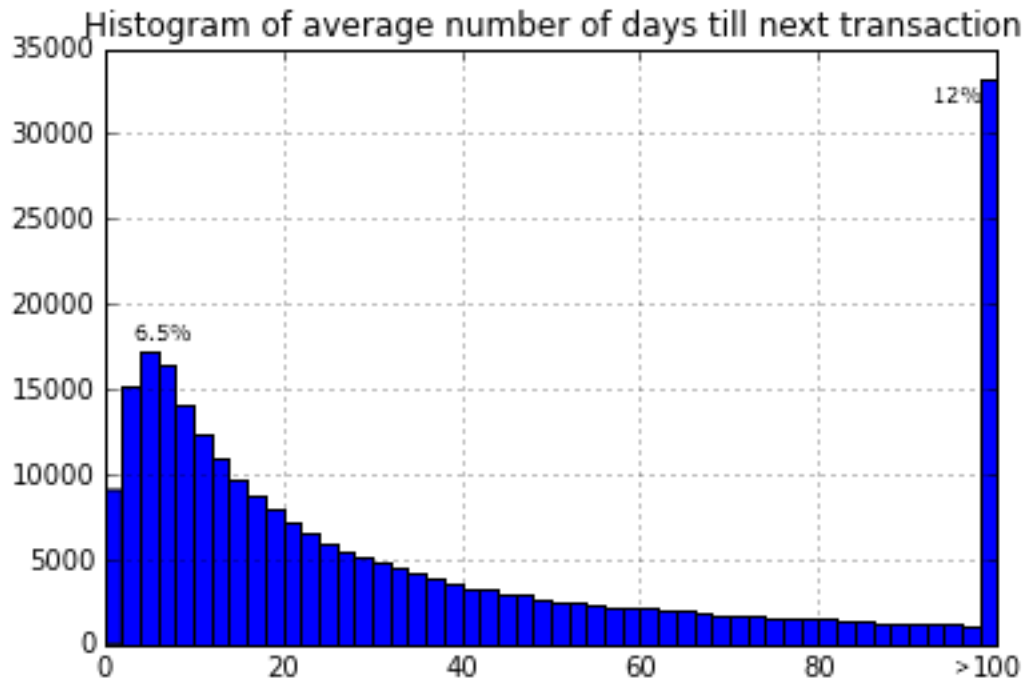


Figure 16. A histogram of the average wait time for the 74% of sampled users with 5 or more public transactions, to publicly conduct a new transaction. To calculate this expected wait I averaged the days between the last 5 visible transactions. All users in the rightmost bin have an average wait of 100 days or more. Forty-seven percent of users are publicly transacting more frequently than once every 20 days. Twenty-one percent are publicly transacting more frequently than once a week, and the modal user is publicly transacting once every 4–5 days.

We can see that most of users with 5 or more public transactions of the site are frequently conducting transactions publicly, with the mode being a public transaction every 4–5 days, and a large fraction (47%) of users having a public payment fewer than every 20 days. A significant percentage of Venmo users (21%) are publicly sharing transaction data at a more frequent rate than once a week in the study's sample, meaning that 2,016,000 people could be leaking a significant amount of private data (assuming the distribution is representative of the entire network and our estimate of 9.6 million users is correct).

Discussion

Venmo publicly displays who is paying whom at what time and for what purpose. This type of data bears a striking resemblance to communication metadata, whose warrantless collection by the U.S. government has been a subject of public and legal debate [24]. As a consequence of Venmo's lack of response to previously identified privacy issues, it is possible that more than 2 million users currently expose large,

potentially intimate parts of their lives and their friends' lives on the platform for the world to see. This is facilitated by Venmo's default sharing behavior and inconsistent, subtle privacy controls. As Venmo expands, these existing privacy vulnerabilities will continue to grow until Venmo changes its policy for handling transaction sharing.

Beyond the privacy issues faced by the 21% of Venmo users who frequently reveal their transactions publicly, there are also security concerns that their data could be used to orchestrate social-engineering attacks against them, tricking them into paying an attacker as described in Kraft et al. in 2014 [10]. For example, if a user pays rent to a roommate via Venmo, an attacker can discern a user's rent schedule, change their own account picture and name to match the roommate's, and then send the user a charge for the rent. These types of attacks are still very possible given that no significant UI change was made to change the practices described by Kraft et al. that make detecting fraudulent transactions difficult [10].

Finally, the data publicly revealed by Venmo about individual users is very easy to gather at scale. Third parties who want to extract a user's public information from Venmo don't even have to make fake Venmo profiles to scrape the data. Because Venmo shows a user's 5 most recent public transactions to any non-authenticated visitor, it would be trivial for a third party to periodically scrape all users' public Venmo pages and generate their full public transaction histories over time.

Venmo can address the privacy concerns demonstrated by this paper, and it has already built some tools to do so. First, Venmo can simplify their privacy settings and set future transactions for users to private or for friends only by default, requiring users to opt into sharing this data publicly. Instead of having two similar-sounding privacy settings, creating a complicated privacy decision tree for each transaction, Venmo can combine the two settings into one "Default audience" setting that would defer to the more restrictive option of the two users in a transaction (i.e., if one user had a Default audience of Public and another user wanted Private, then transactions between the two users would be by default private, regardless of who initiated the transaction). Second, Venmo can make it easier for users to reset all of their past transactions from Public to Private at once rather than one-by-one for each transaction. Venmo has already implemented this in the iOS app (Figure 17) and on Venmo.com as of October 2015, though the feature is not currently available for users of the Android app (as of Version 6.18.1). Finally, Venmo can implement some of the UI changes suggested in Kraft et al. to mitigate social-engineering attacks against users who share a lot of their transaction data publicly [10].

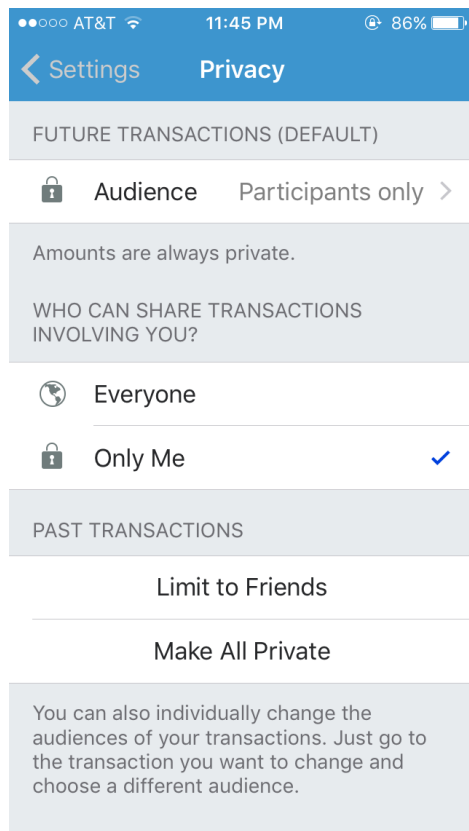


Figure 17. A screenshot of the iOS Venmo app privacy settings. The iOS app allows users to change the visibility of past transactions from Public to Friends or Private.

It remains to be seen whether Venmo will find it in the best interest of the company to amend their sharing features to make hiding transaction activity easier, as social proof has seemed to be an integral part of their growth model. In a 2015 video Venmo's growth lead stated that showing prospective users recent public payments instead of a static screen led to a 20% increase in conversions from app opening to sign-up, and showing users that their friends were transacting on Venmo helped increase engagement with the platform [25].

Drawing on results from my previous research on the collection of geolocation data by Facebook Messenger, Venmo is behaving similarly to Facebook in its lack of response to previously identified privacy vulnerabilities as it balances user and feature growth with security and privacy [26].

While Venmo has already faced regulatory scrutiny in California [12], the broader question raised by this work is whether we can continue to rely on existing regulatory methods to ensure that user data on platforms such as Venmo has an appropriate and expected degree of privacy protection.

Assessment of Methods

The main shortcoming of the analysis done in this paper is the possibly skewed and relatively small sample set of 357,177 users that I identified in my scrape of public profiles.

The breadth-first nature of the sampling and the fact that it was seeded by my own Venmo network, as well as the limit of collecting only the 5 most recent public transactions per user sampled, means that the dataset analyzed here may not be representative of the entire Venmo user population. However, because no list of user profiles is available to randomly draw from, starting the crawls from sets of seed profiles in separate friend clusters provided a methodology to draw from semi-independent subsets of the Venmo population to minimize sampling bias. In addition, because the individual profiles I analyzed with the extension were drawn from my second-degree connections, which served as a seed for the breadth-first search that generated part of the dataset, if anything the bias in the usage data is consistent with the bias in the usage patterns discovered via the extension, though this may not be representative of Venmo as a whole.

Areas of Further Research

Future research into Venmo users' usage patterns should consider network analysis of the social graph to ensure profiles sampled are truly random and representative of the entire population of users. Furthermore, given a longer time frame to collect data, more than the 5 most recent public transactions at a single point in time can be logged for each user to provide higher-resolution data. This can be done by making possibly rate-limited, authenticated requests to the newsfeed API endpoint for each user to get back their entire public history, or periodically scraping users' 5 most recent transactions from their public profiles to generate a history of their activity over time. With higher-resolution data, research can characterize the public transactions indicative of specific activities, such as commercial transactions or gambling, and then comb the network to estimate how many users are using the app for each activity.

Future research can also work to identify cliques of friends who tend to spend money together as well as the analyze dynamics of financial ties within these friends groups. To this end the bubble graph visualization of the Money Trail tool I built, which currently displays star graphs, could be extended to show more expansive social graphs built from transaction histories between multiple users beyond the central user.

References

1. Rose J. Data Privacy by the Numbers. BCG Perspectives. February 19, 2014. https://www.bcgperspectives.com/content/Slideshow/information_technology_strategy_digital_economy_data_privacy_by_the_numbers/#ad-image-3
2. Electronic Code of Federal Regulations. Title 16, Chapter 1, Subchapter C, Part 313. <http://www.ecfr.gov/cgi-bin/text-idx?SID=b51fa477ee4ea9c91a2360eb9c000cfe&mc=true&node=sp16.1.313.b&rgn=div6>
3. Bitcoin. Protocol Documentation. https://en.bitcoin.it/wiki/Protocol_documentation
4. Paypal. Privacy Policy. https://www.paypal.com/webapps/mpp/ua/privacy-full#How_We_Share_Personal_Information_with_Other_Third_Parties
5. Wortham J. After 2 Years of Testing, Venmo Opens Payment Service to Public. New York Times. March 20, 2012. <http://bits.blogs.nytimes.com/2012/03/20/after-2-years-in-beta-venmo-opens-payment-service-to-public/>
6. Adding Multimedia, Ebay Inc. to Acquire Global Payments Innovator Braintree. BusinessWire. September 26, 2013. <http://www.businesswire.com/news/home/20130926005611/en/eBay-Acquire-Global-Payments-Innovator-Braintree#.ViBQYBNViko>
7. Heggstuen J. Venmo Payment Volume Reaches Nearly \$1 Billion, But Growth Is Slowing. LinkedIn Pulse. February 2, 2015 <https://www.linkedin.com/pulse/venmo-payment-volume-reaches-nearly-1-billion-growth-john-heggstuen>
8. Constine J. Can Paying Friends Be Fun? Venmo Features “News Feed of Payments” In Redesigned App. Tech Crunch. June 5, 2012. <http://techcrunch.com/2012/06/05/venmo/>
9. Venmo. How do I keep my payment activity private? <https://web.archive.org/web/20150915122203/https://help.venmo.com/customer/portal/articles/1322627-how-do-i-keep-my-payment-activity-private->
10. Kraft B, Mannes E, Moldow J. Security Research of a Social Payment App. MIT. May 14, 2014. <https://courses.csail.mit.edu/6.857/2014/files/13-benkraft-jmoldow-mannes-venmo.pdf>
11. AllMyChanges.com. iOS/Venmo's Changelog. <https://allmychanges.com/p/ios/Venmo/>

12. Owen J. Venmo Inc Final Order. State of California Department of Business Oversight. June 21, 2014.
http://www.dbo.ca.gov/Laws_&_Regs/dfi_orders_files/2014_Venmo_Final_Order.pdf
13. Griswold A. Venmo Money, Venmo Problems. Slate. February 25, 2015.
http://www.slate.com/articles/technology/safety_net/2015/02/venmo_security_it_s_not_as_strong_as_the_company_wants_you_to_think.html
14. Lecher C. Venmo's Two Factor Authentication System Launches Today. The Verge. April 2, 2015. <http://www.theverge.com/2015/4/2/8334385/venmo-two-factor-authentication-launches>
15. Griswold A. Venmo Scammers Know Something You Don't. Slate. September 15, 2015.
http://www.slate.com/articles/business/moneybox/2015/09/venmo_scam_and_fraud_why_it_s_easy_to_get_ripped_off_through_the_mobile.html
16. Vicemo. <http://www.vicemo.com/>
17. D'Onfro J. Vicemo Lets You See Who Is Buying Drugs and Sex on Venmo. Business Insider. February 3, 2015. <http://www.businessinsider.com/vicemo-lets-you-see-who-is-buying-drugs-and-sex-on-venmo-2015-2>
18. Dewey C. Why Would Anyone In Her Right Mind Use Venmo. The Washington Post. February 26, 2015. <https://www.washingtonpost.com/news/the-intersect/wp/2015/02/26/why-would-anyone-in-her-right-mind-use-venmo/>
19. Vaughan M. A Note to Our Venmo Community. Venmo. February 27, 2015.
<http://blog.venmo.com/hf2t3h4x98p5e13z82pl8j66ngcmry/2015/2/27/a-note-to-our-venmo-community>
20. arankhanna25. Marauders Map. Chrome Web Store. October 22, 2015.
<https://chrome.google.com/webstore/detail/money-trail/pfapkinkogbekmajdmmdiificmnkeflm?authuser=1>
21. arank. money-trail. Github. October 22, 2015.
<https://github.com/arank/money-trail>
22. Cao J. Millennials Say 'Venmo Me' to Fuel Mobile-Payment Surge. Bloomberg. August 18, 2014. <http://www.bloomberg.com/news/articles/2014-08-18/millennials-say-venmo-me-to-fuel-mobile-payment-surge-tech>

Khanna A. Venmo'ed: Sharing Your Payment Data With the World. *Technology Science*. 2015102901. September 29, 2015. <http://techscience.org/a/2015102901/>

23. Toplin J, Bakker E. What Venmo's New Segment Could Mean for its Future. Business Insider. August 21, 2015. <http://www.businessinsider.com/venmos-new-segment-and-its-future-2015-8>
24. Peralta E. US Appeals Court Overturns Decision that NSA Metadata Collection Was Illegal. NPR. August 28, 2015. <http://www.npr.org/sections/thetwo-way/2015/08/28/435506021/u-s-appeals-court-overturns-decision-that-nsa-metadata-collection-was-illegal>
25. Mixpanel. Leveraging Social Proof For Growth. May 7, 2015. <https://mixpanel.com/education/leveraging-social-proof-for-growth>
26. Khanna A. Facebook's Privacy Incident Response: A study of geolocation sharing on Facebook Messenger. *Journal of Technology Science*. Harvard University. Cambridge. August 11, 2015. <http://www.techscience.org/a/2015081101/>

Authors

Aran Khanna is a senior at Harvard College majoring in Computer Science joint with Mathematics. During his time at Harvard he has interned at Microsoft, Novus, a hedge fund data analysis startup based in New York City, and Marianas Labs, a deep learning startup based in Mountain View. Aran is an active blogger in his free time and is passionate about the impact the increasing role of technology in our lives is having on our privacy.

Referring Editor: Latanya Sweeney

Citation

Khanna A. Venmo'ed: Sharing Your Payment Data With the World. *Technology Science*. 2015102901. September 29, 2015. <http://techscience.org/a/2015102901/>

Data

Money Trail extension: <https://chrome.google.com/webstore/detail/money-trail/pfapkinkogbekmajdmmmdiifcmmnkeflm>

Khanna A. Venmo'ed: Sharing Your Payment Data With the World. *Technology Science*. 2015102901. September 29, 2015. <http://techscience.org/a/2015102901/>

The code for Money Trail: <https://github.com/arank/money-trail>

The data of public transactions from Venmo used for analysis:
<http://techscience.org/a/2015102801/data/>