



Phoneyptot: Data-driven Understanding of Telephony Threats

Payas Gupta, New York University Abu Dhabi

Bharat Srinivasan, Georgia Tech

Vijay Balasubramaniyan, Pindrop Security

Mustaque Ahamad, Georgia Tech and New York University Abu Dhabi

The Threat

SCAMS

2.6 Billion Robo-Calls Later, Why Won't Rachel from Cardholder Services Just Go Away?

By Mitch Lipka @mitchlipka | April 06, 2012 | 6 Comments

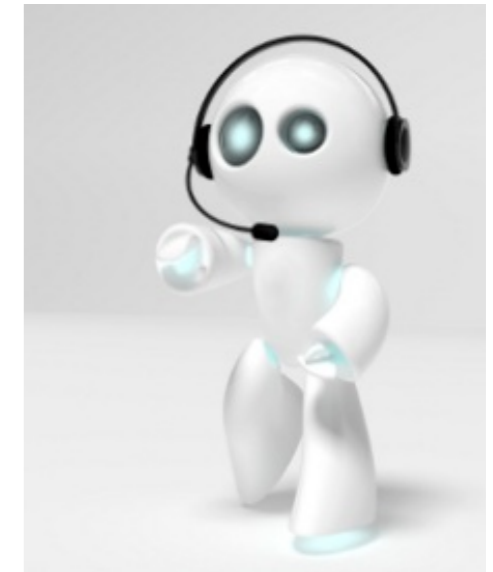
[f Share](#)
[f Like](#) 116
 [t Tweet](#) 1
 [g+1](#) 7
 [in Share](#)
[Pin it](#)
[Read Later](#)

Rachel from Cardholder Services, please stop calling. We all know you're a scam.

If you've never heard from Rachel, consider yourself lucky. Rachel is the name untold millions of Americans have heard when answering their phones with a message that at first appears to be coming from their credit card company. "Hi. This is Rachel from Cardholder Services" is how it usually begins. What follows then is an offer to reduce your credit card rates, and if you follow, you'll likely be paying for the price



Getty Images



The Threat



Robert Siciliano ♥ Become a fan
Personal Security and Identity Theft Expert

✉ RSS Follow Like 33

FTC: Tech Support Scams are baaaaack!

Posted: 02/05/2014 1:31 pm EST | Updated: 02/13/2014 12:59 pm EST

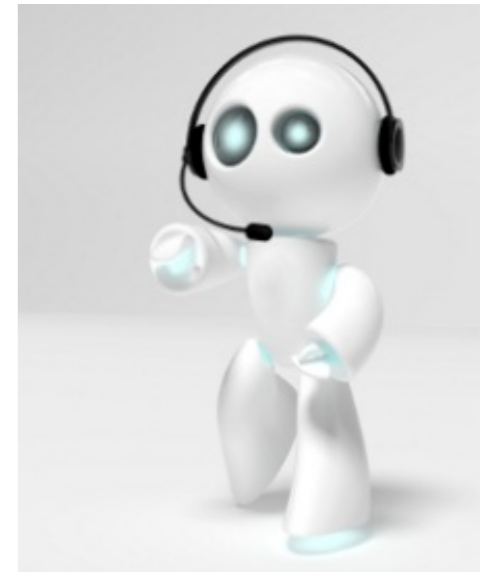


7	5	10	submit	0	0
Like	Share	Tweet	reddit	Email	Comment

su f t g+

MORE: Crime, Scams, Identity Theft, Hacking, Scams, Privacy, Scamming, Hackers, Identity Protection, Crime News

They're back, and they're scarier than fangy blood sucking ghosts: tech support scammers. They want to suck you dry of your last penny.



Understanding the Threat: Current Data Sources

- Telcos
- Crowd sourced
 - FTC, CRTC complaint datasets
 - 800notes open datasets
- Proprietary

Dataset Requirements: ACT

- Accuracy
- Completeness
- Timeliness

Problems with Current Data Sources

- A - Accuracy

909-693-3689

Did you get a call from 9096933689? Read the posts below to find out details about this number. Also [report unwanted calls](#) to help identify who is using this phone number.

909-693-3689

Country: USA

Location: California (Anaheim, Chino, Diamond Bar)



Annoyed Victim

1 h 27 min ago



0



I have received probably 30 calls to my cell phone from this number. Never leaves a message. It's truly annoying. I have no idea who or where this person is calling from and can only assume it's a scam!

Caller: No idea

Reply

!

Report a phone call from 909-693-3689:

Your Name *

Your name as you would like it to appear in the title of your post.

Message *

No Actual Timestamps

- Reported as “calls for hours” now

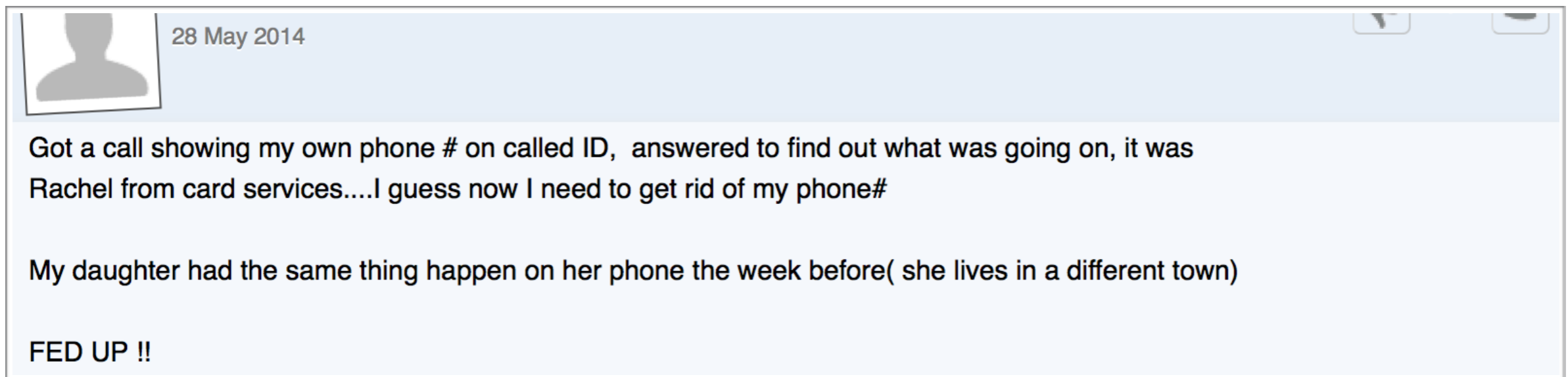
Been getting these calls for hours now. I tried to unsubscribe but the phone call drops three digits into my cell phone number. I only answered twice. It was the same lady 'Ashley' I hung up the first time. The second time I answered, I told them to stop calling me right now. She immediately hung up. I haven't been called since, but it usually only happens once an hour so they may call back.

Caller: Academic Advisor.

Call Type: Survey

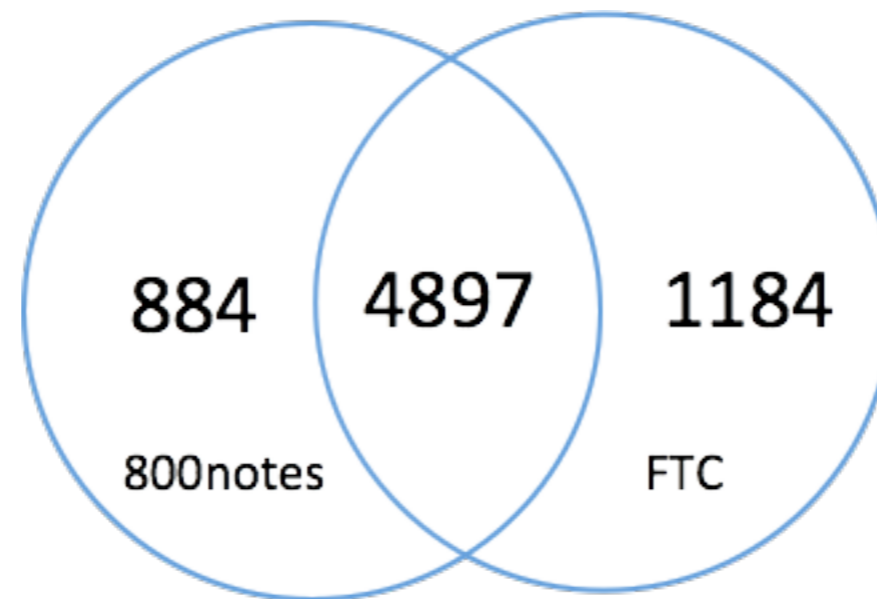
Spoofting

- Caller number same as callee number



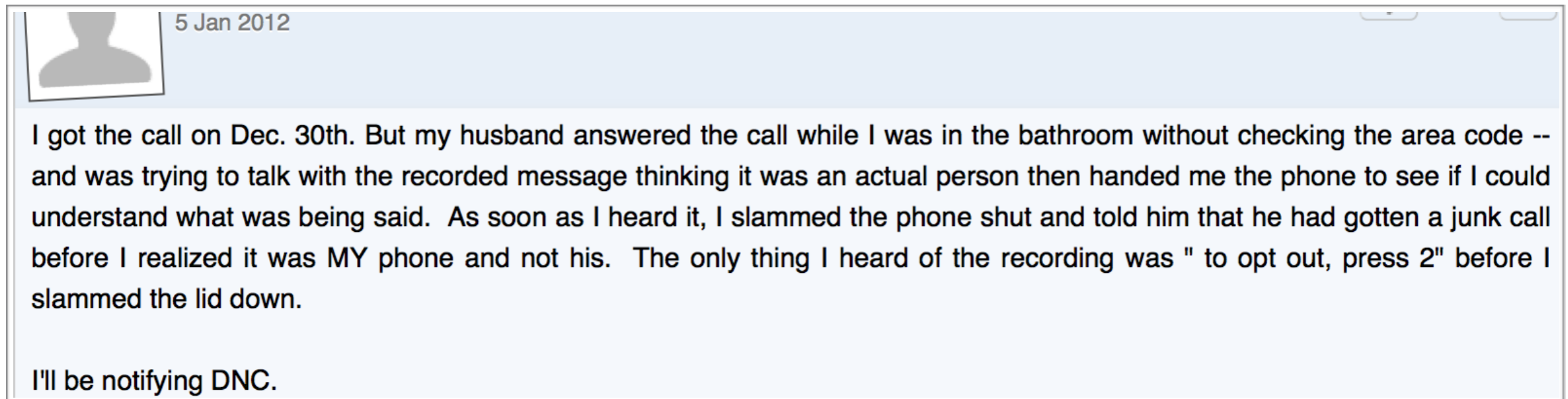
Problems with Current Data Sources

- C - Completeness
 - Compared both FTC and 800notes against each other for a certain set of numbers



Problems with Current Data Sources

- T - Timeliness



5 Jan 2012

I got the call on Dec. 30th. But my husband answered the call while I was in the bathroom without checking the area code -- and was trying to talk with the recorded message thinking it was an actual person then handed me the phone to see if I could understand what was being said. As soon as I heard it, I slammed the phone shut and told him that he had gotten a junk call before I realized it was MY phone and not his. The only thing I heard of the recording was " to opt out, press 2" before I slammed the lid down.

I'll be notifying DNC.

Phoneypot



Phoneytokens

- Phoneytokens are digital piece of information (*phone numbers + features* in our case) whose value lies in the unauthorized use of these token.
- Features
 - Age
 - Profile
 - Geography

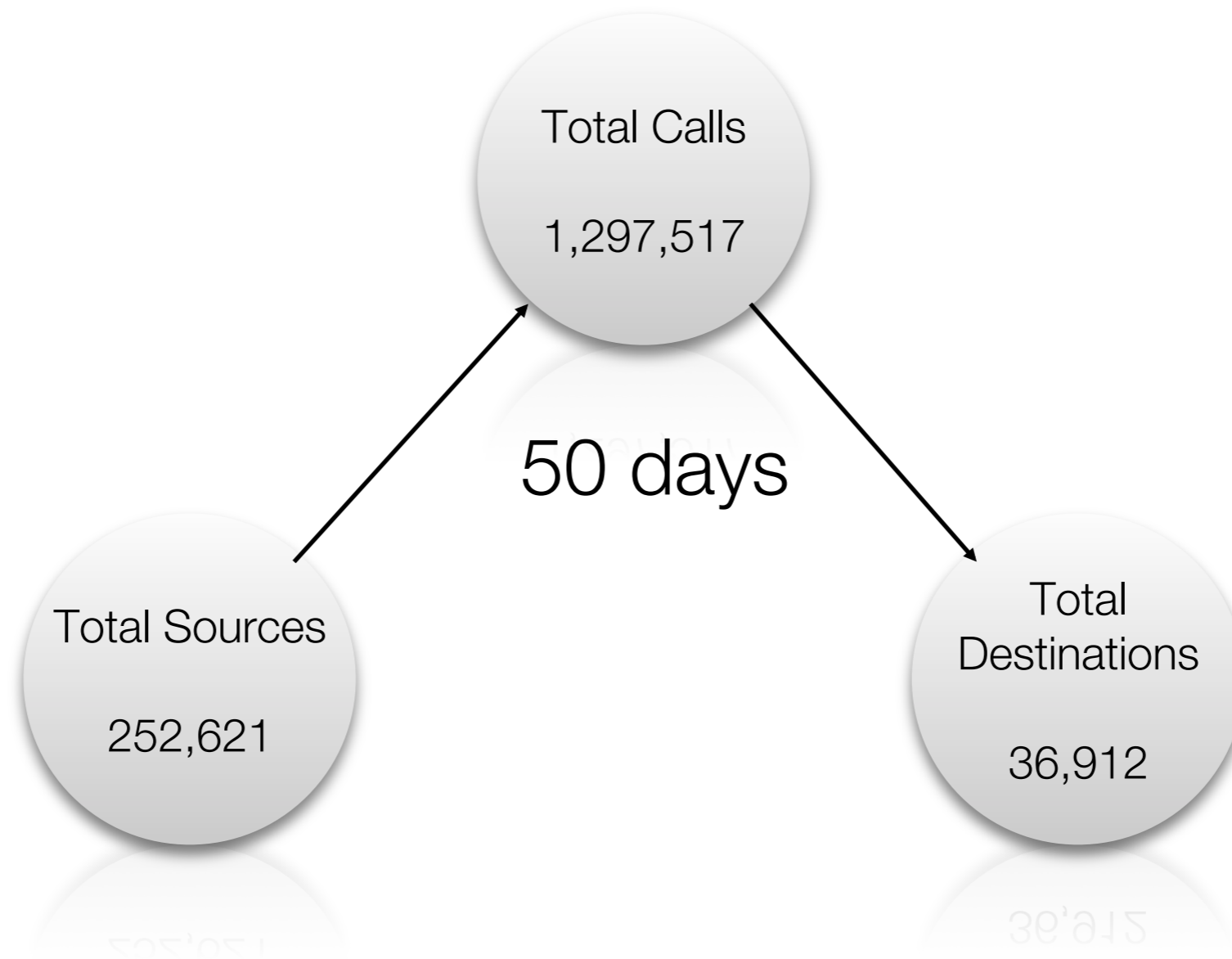
Challenges

- Anonymously pushing phoneytokens
- Ability to engage callers
- Automation
- Legal: Telephone conversation recording laws
- Dealing with false positives
- Cost
- Ethics

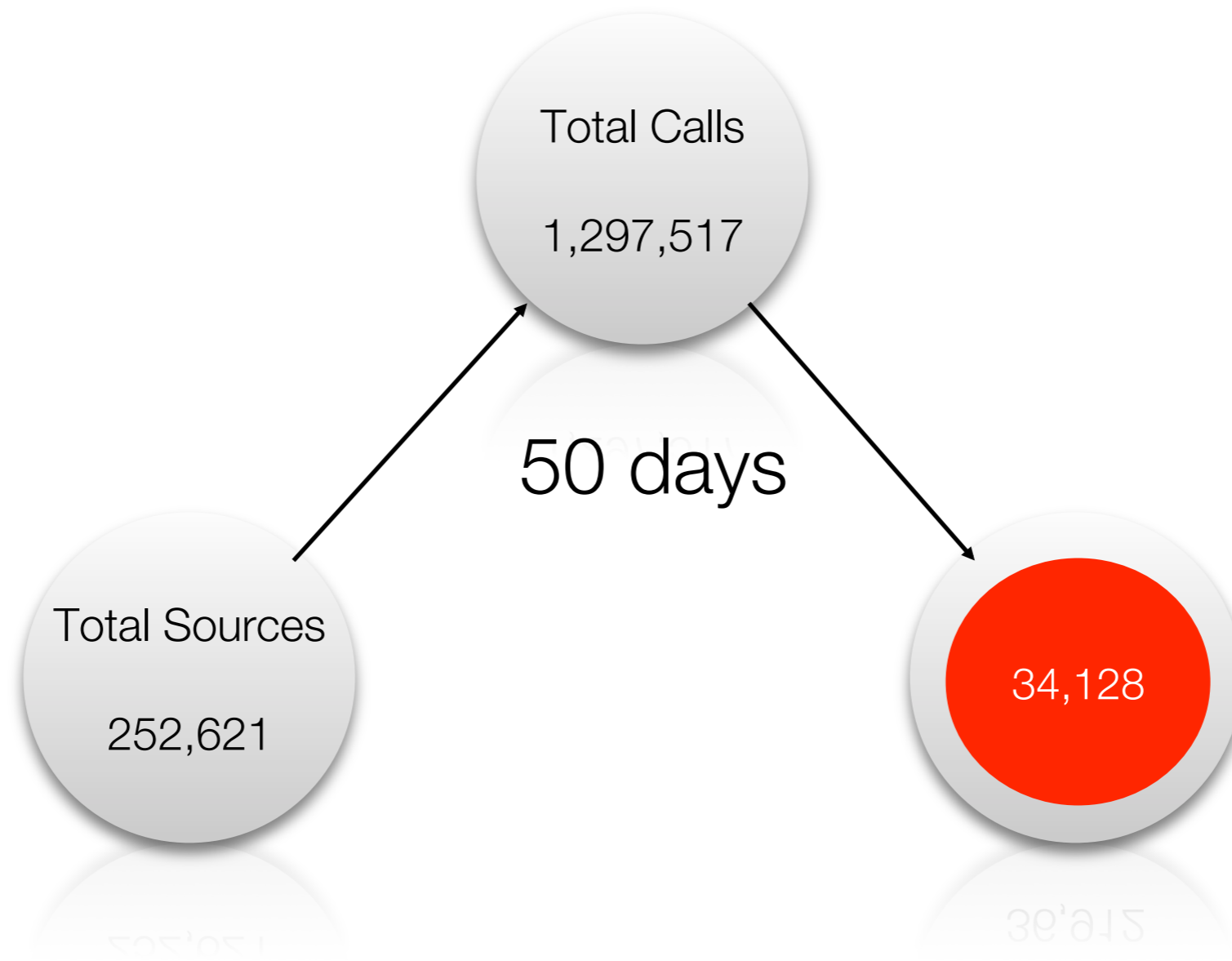
Experiment Settings

- 36,000 dirty phoneytokens from a Telco
- Did not seed these phoneytokens
- Call duration of 2 seconds and then hang up
- Did not record or pick up any of the calls

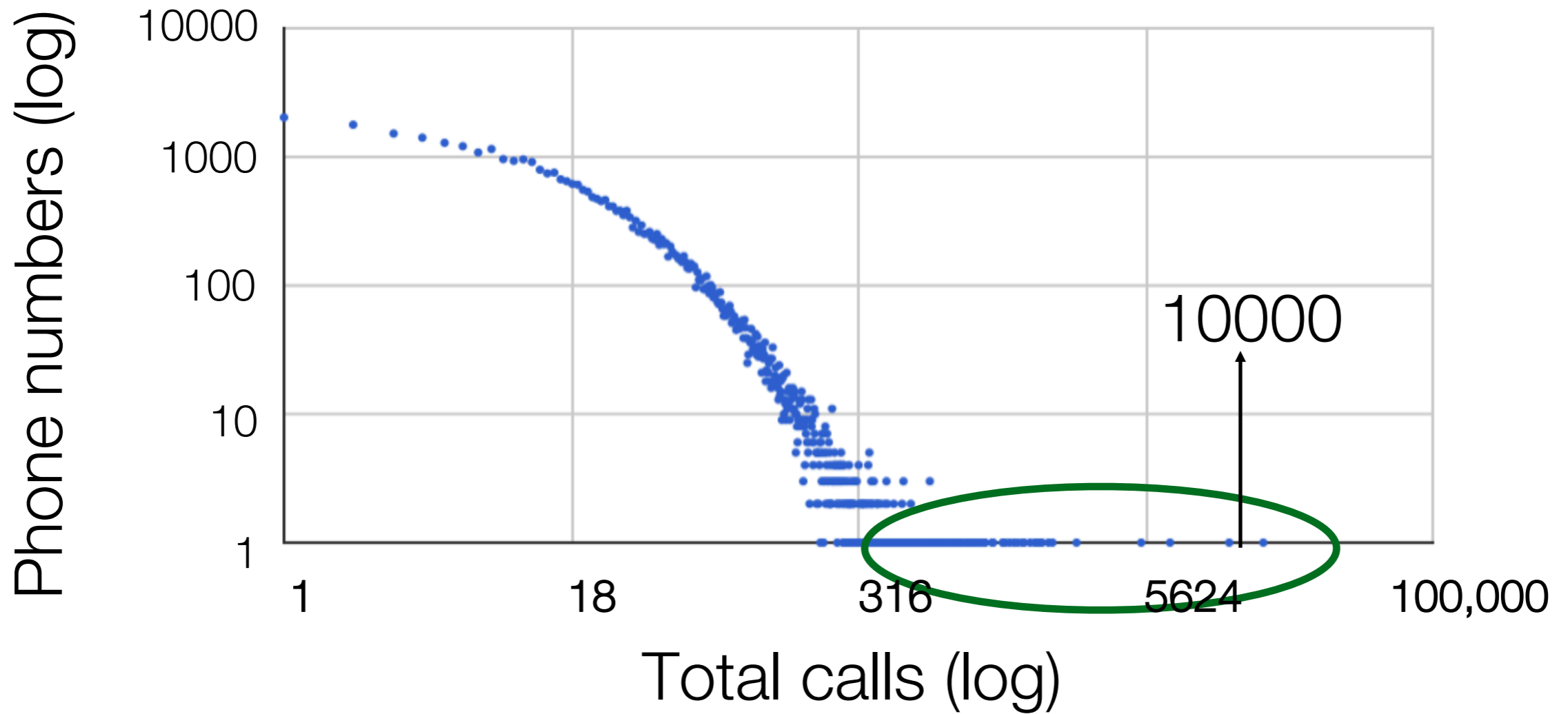
Initial Results



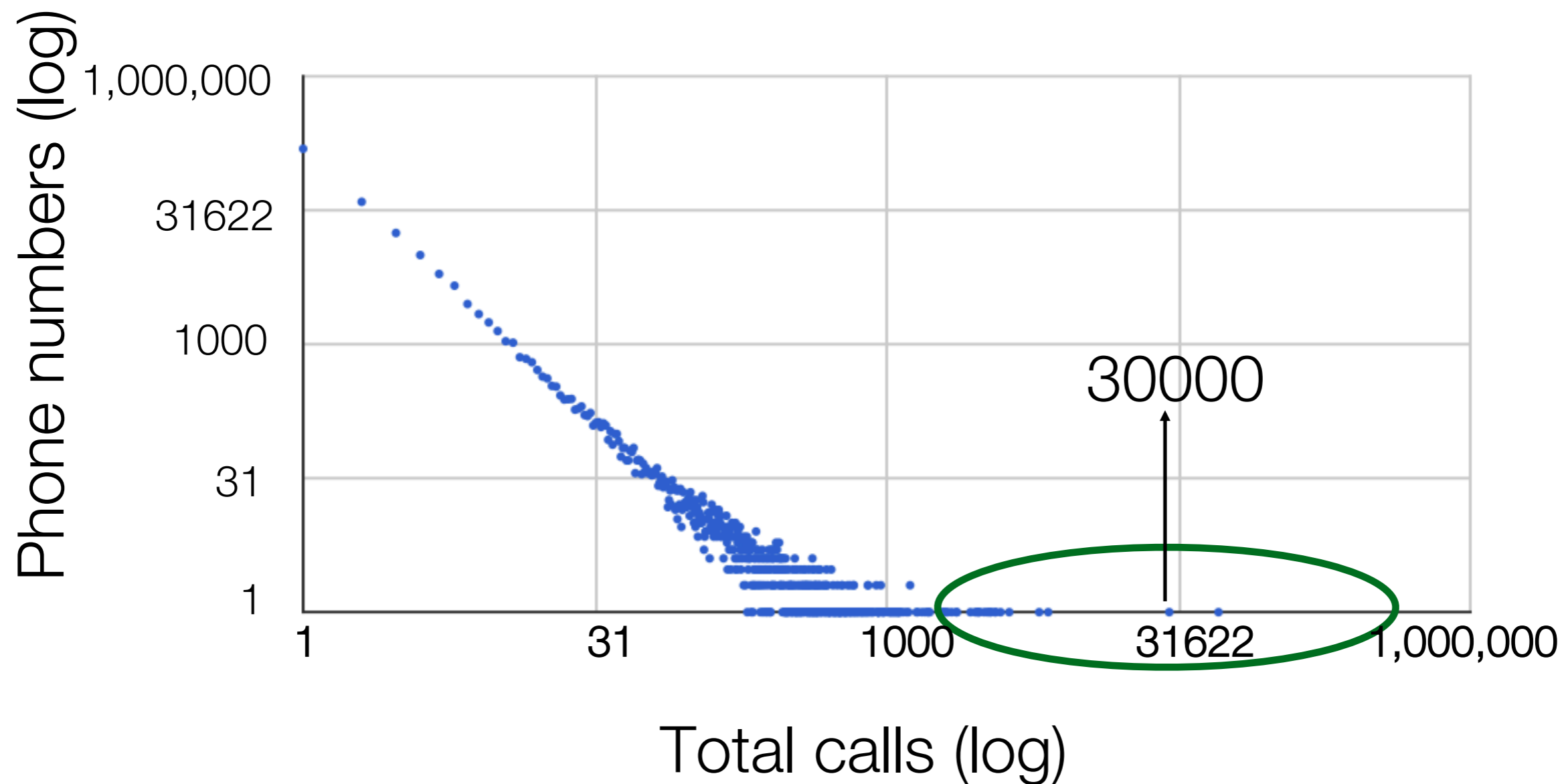
Initial Results



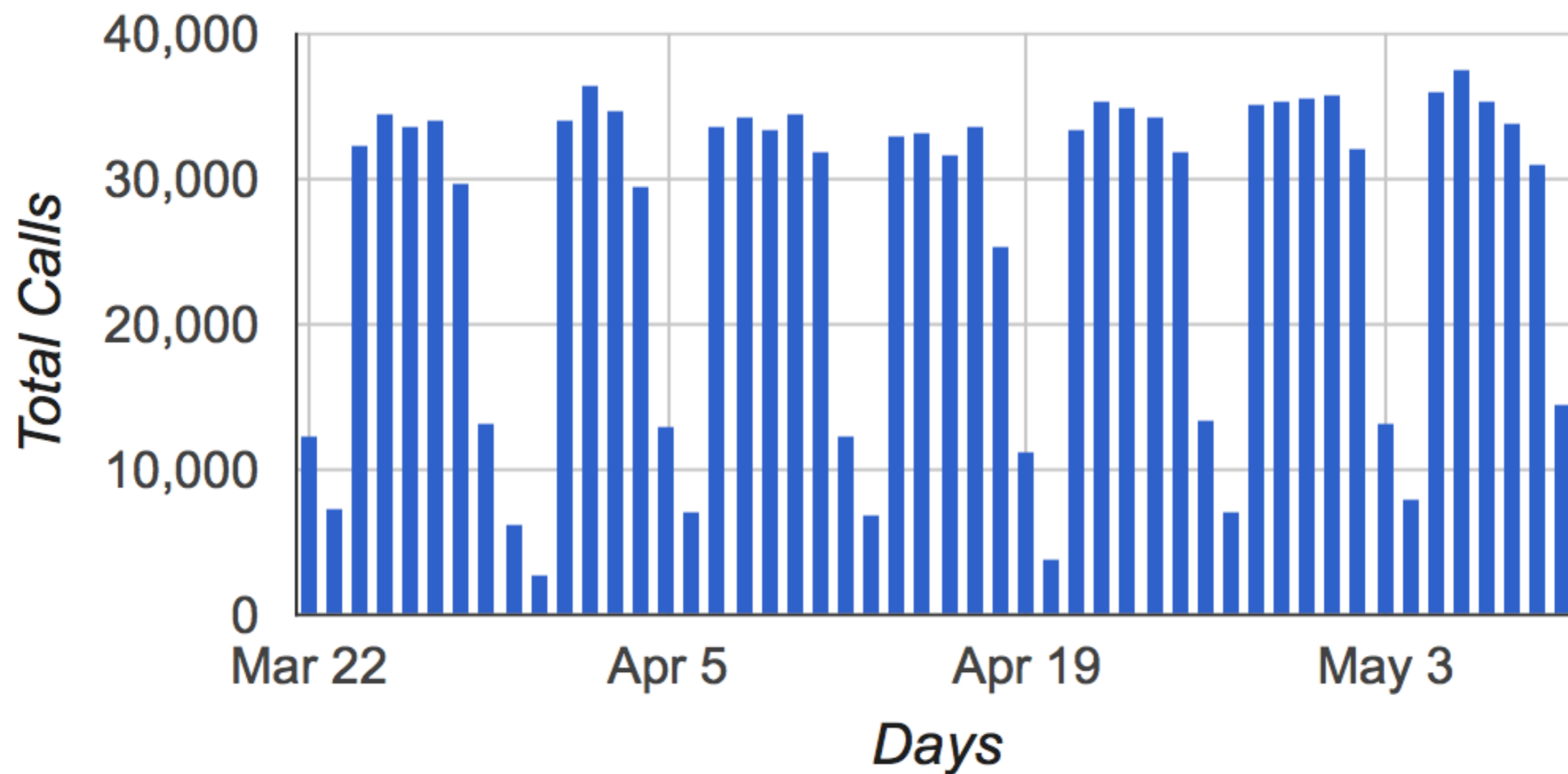
Destination Numbers Distribution



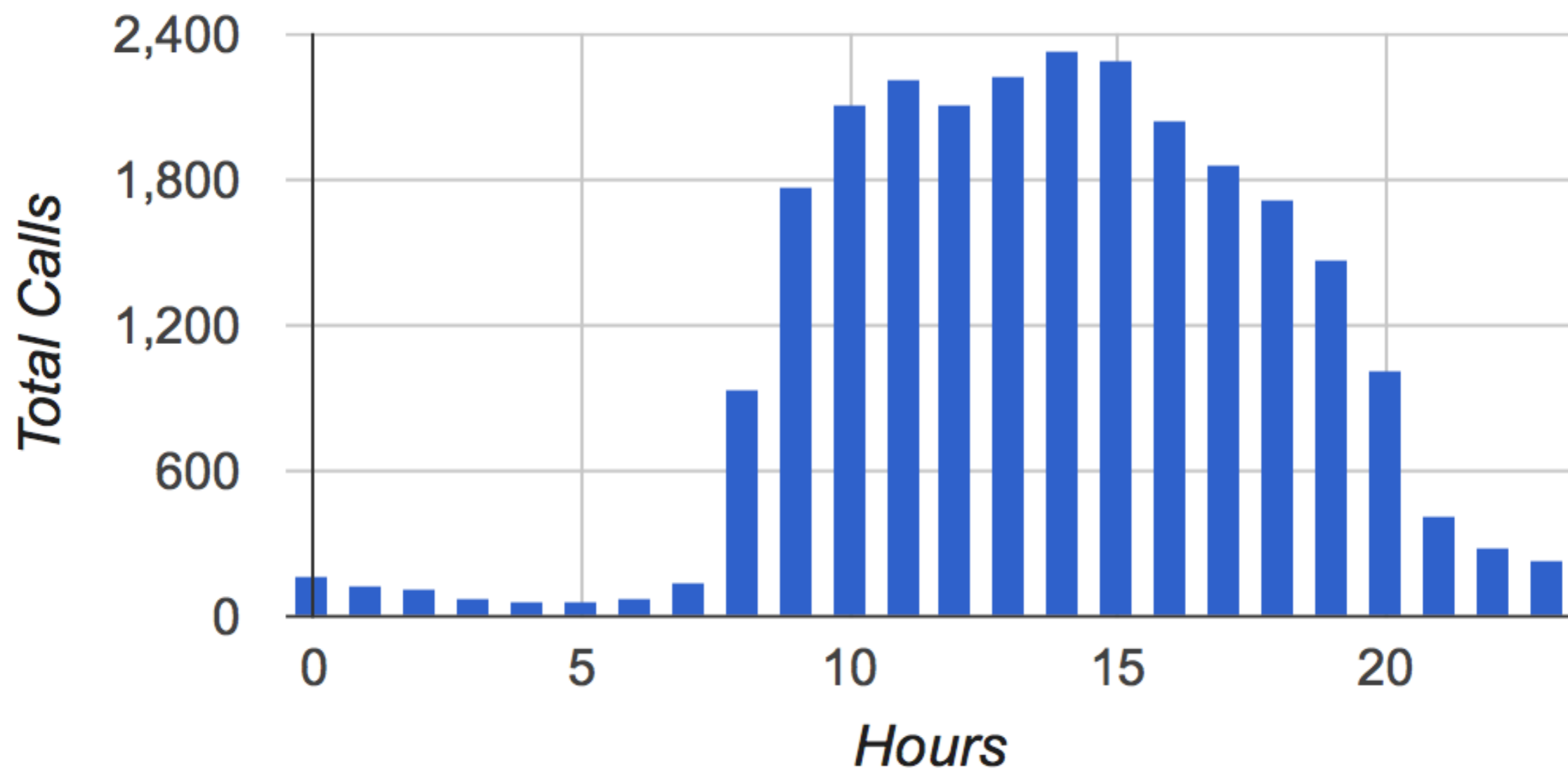
Source Numbers Distribution



Daily Call Volume

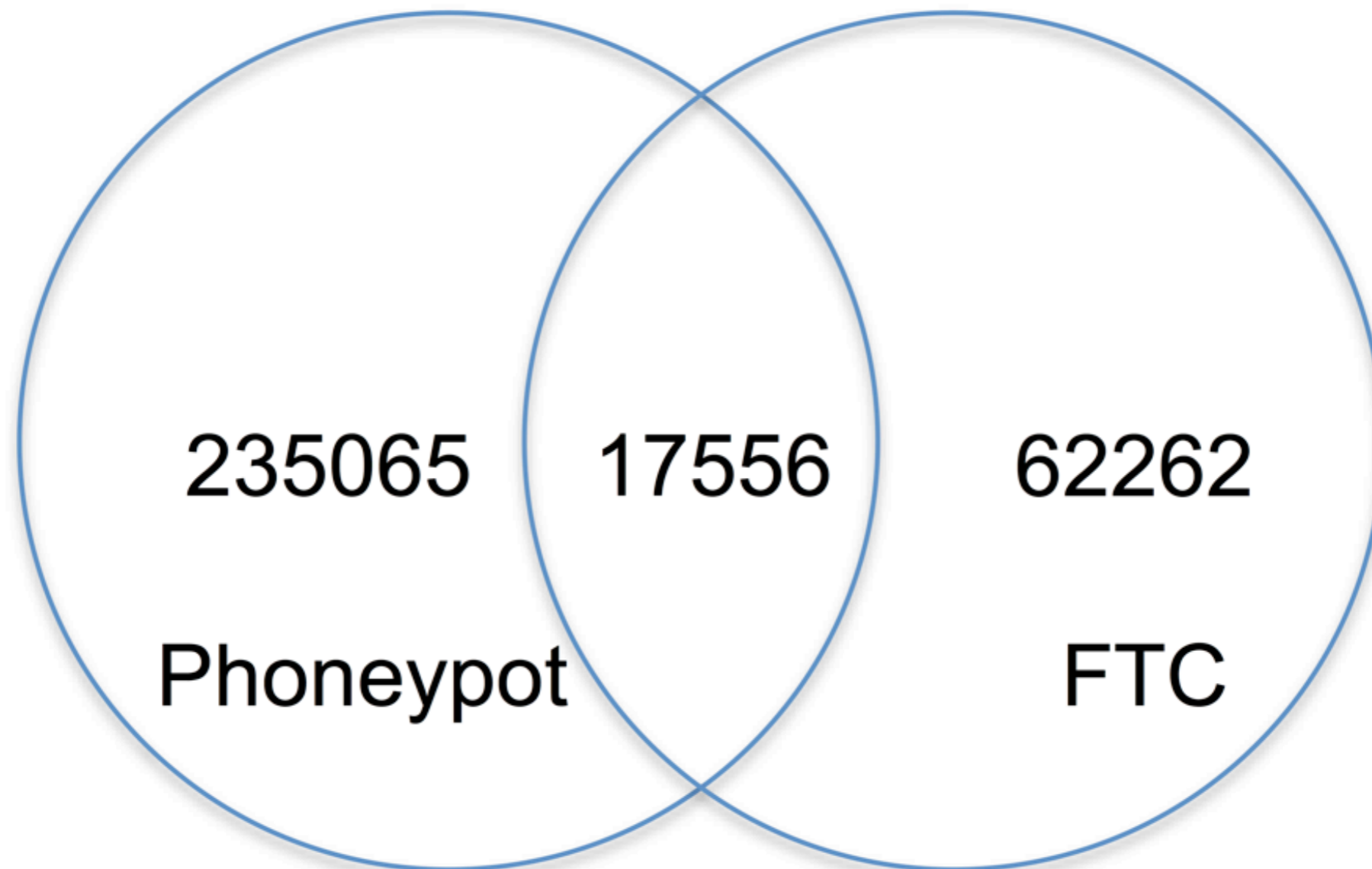


Hourly Call Volume



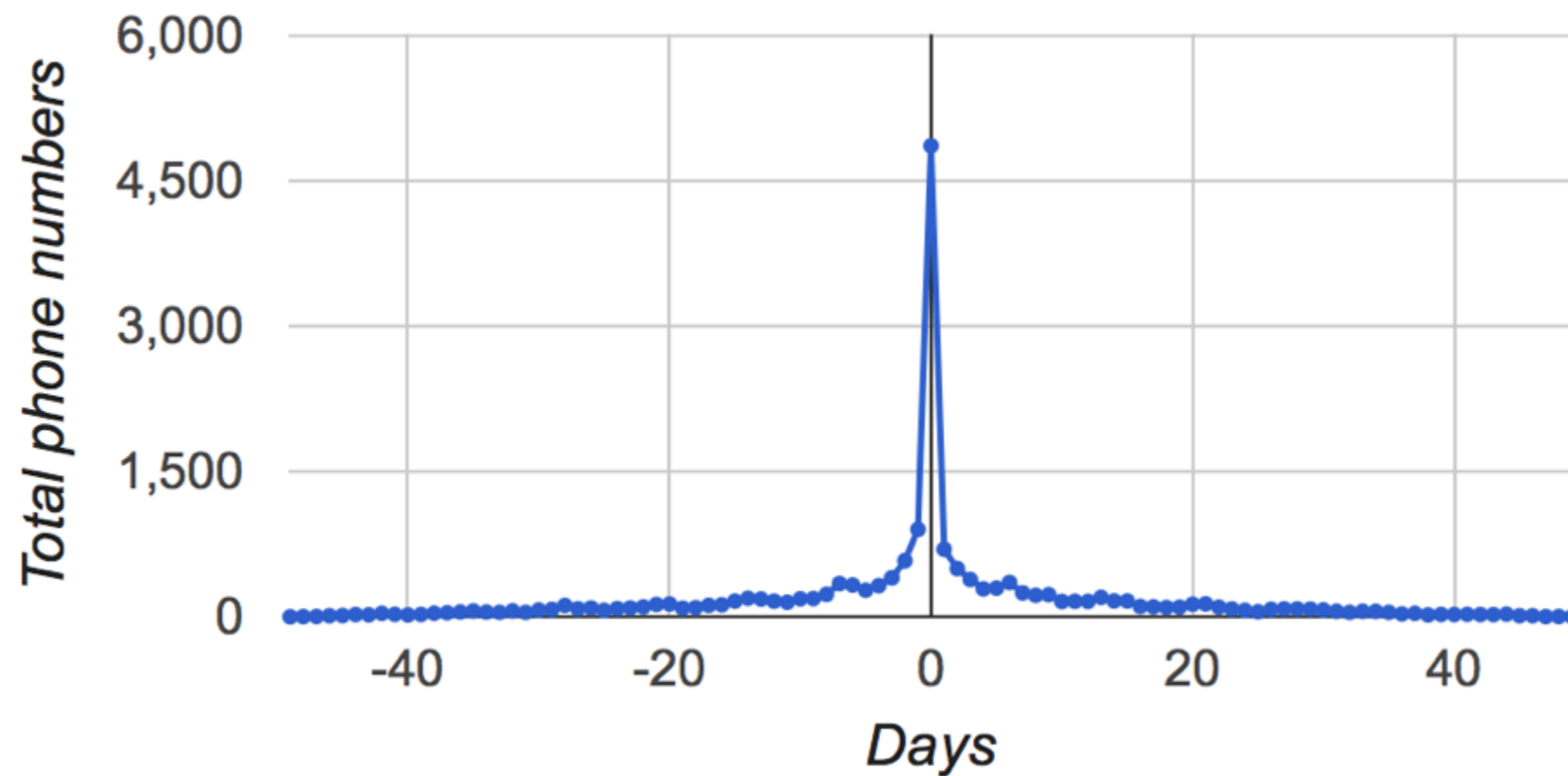
Evaluation of Honeypot on ACT principles

- C - Completeness



Evaluation of Honeypot on ACT principles

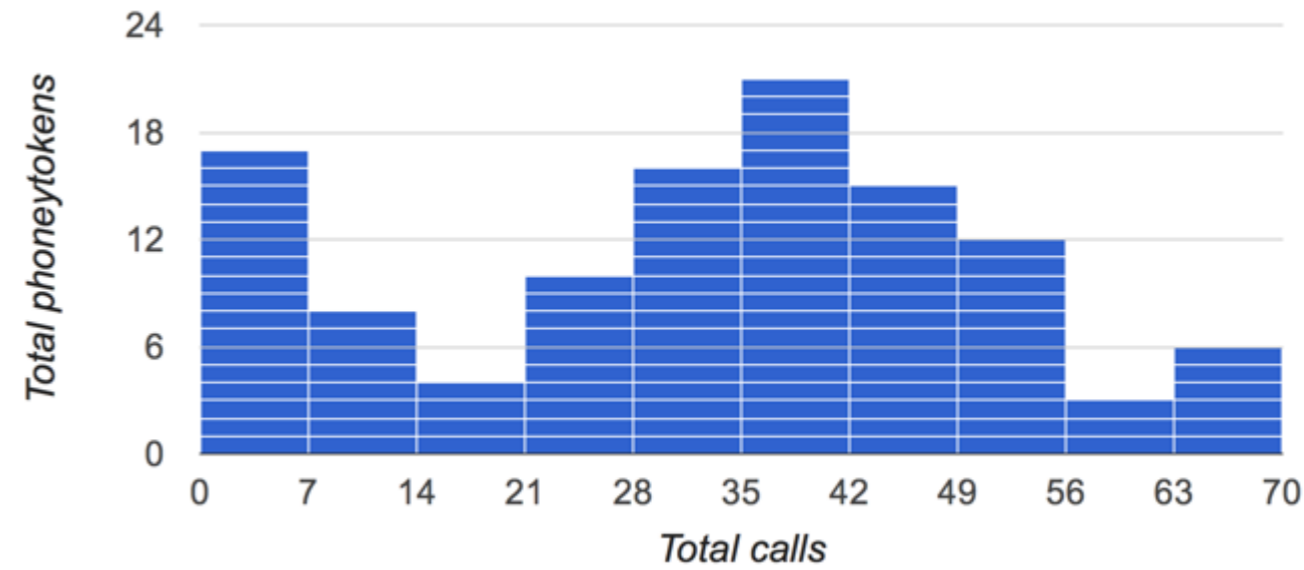
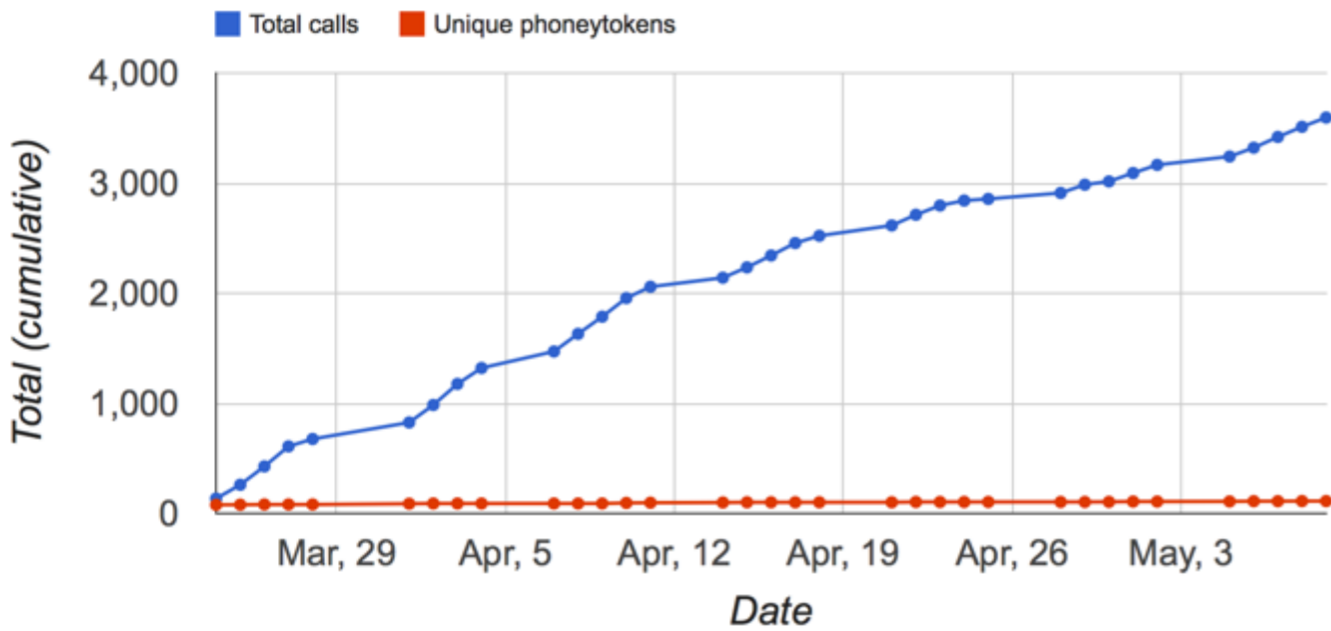
- T - Timeliness



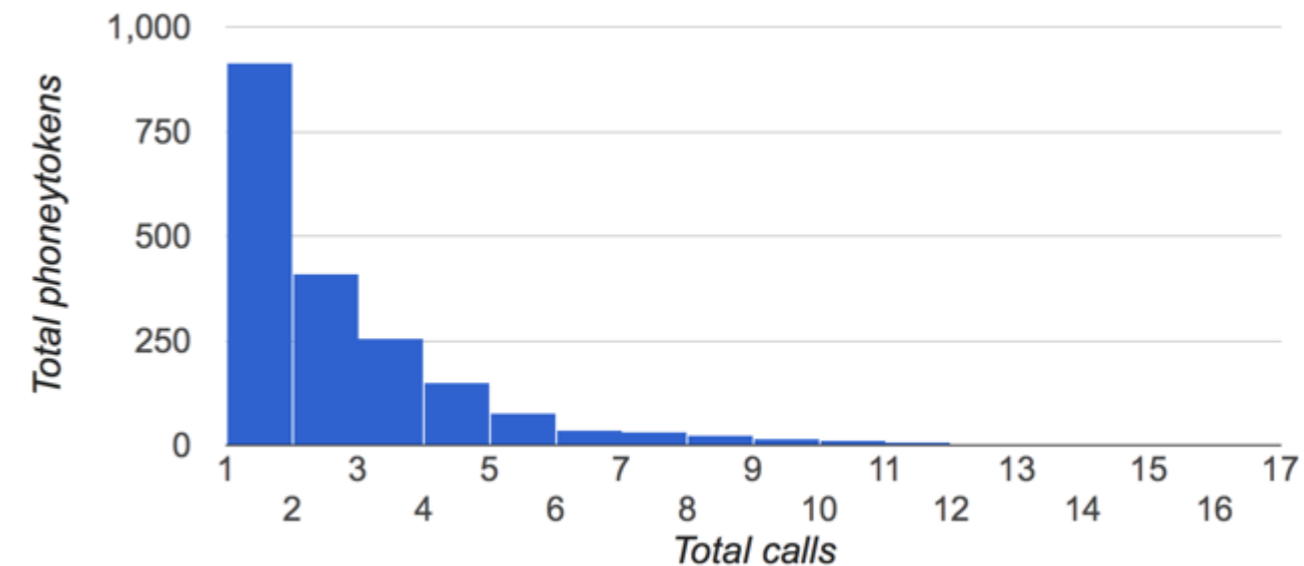
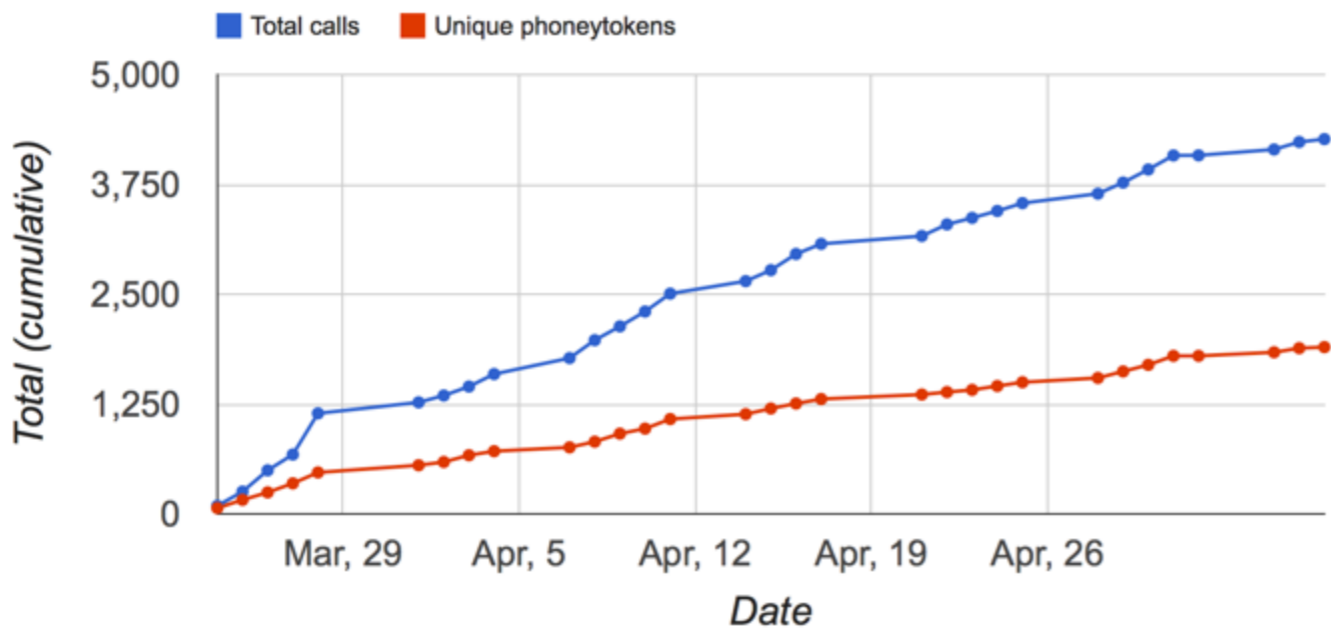
Noticeable Calling Patterns

Debt Collector v/s Telemarketer

Debt Collector



Telemarketer



Allied Interstate Debt Collector

FDCPA - Fair Debt Collection Practices Act

Florida Lawyer Fighting Debt Collection Abuse, Harassment, Calls, & Debt Collector Lies

CATEGORIES

[Attorney General \(2\)](#)

[Bankruptcy \(5\)](#)

[Banks \(7\)](#)

[Collection Agencies \(123\)](#)

[Collection Calls \(9\)](#)

[Collection Lawsuits \(13\)](#)

[Collection Lawyer \(4\)](#)

[Collection Methods \(4\)](#)

Allied Interstate Settles — Agrees to Pay \$ 1.75 Million Fine

by DONALD PETERSEN on DECEMBER 11, 2010

On October 22, 2010, Allied Interstate agreed to pay a fine totaling \$ 1,750,000 to settle the FTC's allegations that Allied violated the FDCPA while attempting to collect accounts from consumers during 2006 through 2008. The \$ 1,750,000 fine is the second largest that a debt collector has agreed to pay the FTC.

Summary

- Can be used to collect better intelligence about telephony attacks
- That there were many instances where honeypot received calls from fraudulent phone numbers before it was reported on the other datasets.
- Can complement current data collection mechanisms
- Noticeable calling patterns like telemarketer, debt collectors etc. can be observed from the datasets.

Open Challenges and Questions

- How many numbers do we need for completeness?
- Understanding how numbers are chosen/qualified?

Thanks

Payas Gupta

Email - payasgupta@nyu.edu