Analyzing Peer-to-Peer Online Social Networks
Agenda

• Background
• Introduction
• Related Work
• Conclusion
Background
Problems

• Unfair rules which change all the time without consent
• Ex: Instagram’s TOC change
Problems

• Privacy? What Privacy?
  – Obscure privacy controls.
  – Unintended consequences of actions.
  – Ex: Tagging a person in a private picture
  – Ex: Giving access to an app

• Equivocation or censorship by the provider
  – WYS – N – WIS

• If it can be seen, It’ll be seen
Problems

- Stored for eternity
- No fair access to data
- Single point of failure
- Fear of the “Big Brother”
- Security is not inherent
Solution

• Peer-to-Peer social networking
What is P2P social networking?

- Nodes interact with each other directly
- Full control over data
- End-to-End encryption
- Minimal central management
- No single view of the entire graph exists
- No central control
Why now? - Technology

• Duh! Moore’s law!
• Thick clients
• Even datacenters run on commodity servers
• Faster internet connections
• Cost of an always-on node in a datacenter is affordable by many
Why now? People

• There “may be” latent demand
• After being “violated” many times, people understand privacy now
• Tired of government oversight
• Uncomfortable with data breaches
But, Why?

- Peer to Peer systems genuinely solve problems
- Reduce attack surface
- Greater control over data
- Privacy will finally be in our hands
What has been done?

• Various groups proposed different architectures
• Mostly research projects
• Despite being P2P, no implementation available
• Most studies try to implement features of current social networks
Core Ideas
Core Ideas

• People passing messages
  – ONE to MANY
  – ONE to ONE

• Different classes of relations
  – FRIEND
  – FOLLOWER

• Different types of messages
  – TEXT, PHOTO, VIDEO
Core Ideas

• If a P2P system can implement these core ideas, all the other features can be taken care at the client level
Topic

• Analyze various network configurations to support the core ideas outlined before
• Analyze features that can be built on top
• Analyze metrics and check feasibility
Friendtegrity - Ideas

- P2P with a central provider
- Storage is at the provider but is assumed to be untrusted
- Stored data is encrypted
- Core concept is to avoid equivocation
- Detects misbehavior
- Peers speak among themselves to confirm the view presented by the server
• Provider can deduce an anonymous graph of relations between peers
• Adopting a central server defeats the purpose of P2P
  – Monetization issues
  – Single point of failure

Friendtegrity - Issues
Safebook

• Goals are Privacy, Integrity and availability
• Matryoshkas to leverage real life trust for use in the network
• Peer to Peer substrate to provide data lookup
• Central Trusted identification service
• Need invitation from existing members
• Good at anonymizing the flow of data
PeerSoN

- Supports offline transactions
- Two tier system
- DHT based lookup service to service clients on resource constrained devices
- Can use existing DHT networks
PeerSoN

- Peers and user data in another tier
- Encryption to mask data
- Messages can be passed asynchronously
Cachet

• High number of lookups in traditional DHT adds to latency
• Can run into hundreds of seconds
• To solve latency issues with stock DHT implementations
• DHT augmented with social links between users while being base storage
Cachet

• Gossip-based social caching algorithm improves latency
• Peers query online users directly for updates
• If unavailable, DHT retrieves updates that are not cached
Conclusion

• Peer-to-Peer social networking is possible!
• Simulate and analyze a P2P social network
• Understand the features it can support while,
  – Respecting privacy of users
  – Ensuring Integrity of data
  – Availability of the system
Questions