On designing Social Norm Grounded Privacy-preserving Systems

Dr. Mainack Mondal
IIT Kharagpur

CSIRO's Data61, November 2023

My research agenda

Designing, building and auditing systems for managing privacy and security of user data as required by social norms

Privacy violation from real world

- Cambridge analytica scandal
  - Collection of millions of users info via Facebook app
  - Allegedly used in targeting users and affecting election

Privacy violation from real world

- Cambridge analytica scandal
  - Collection of millions of users info via Facebook app
  - Allegedly used in targeting users and affecting election

Privacy violation from real world

- Cambridge analytica scandal
  - Collection of millions of users info via Facebook app
  - Allegedly used in targeting users and affecting election

General expectations about **acceptable data usage** are violated

Privacy violation from real world

- Cambridge analytica scandal
  - Collection of millions of users info via Facebook app
  - Allegedly used in targeting users and affecting election

General expectations about **acceptable data usage** are violated

Social norms are violated

What are social norms?

Social norms are rules developed, by a group of people that specify how people must, should, may, should not and must not behave in various situations

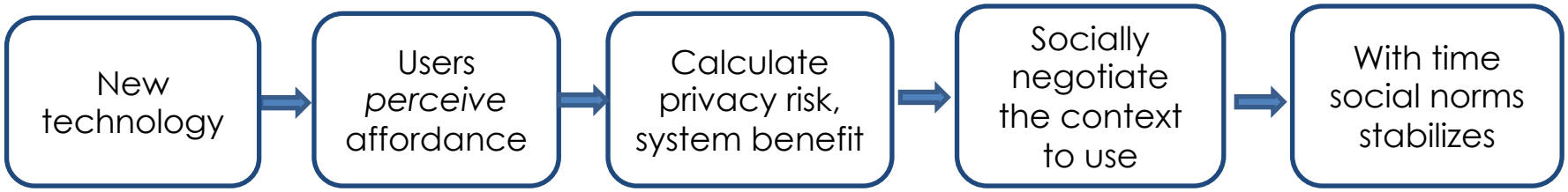
-- *Larson & Goerman*

What are social norms?

Social norms are rules developed, by a group of people that specify how people **and systems** must, should, may, should not and must not behave in various situations

-- *Larson & Goerman*

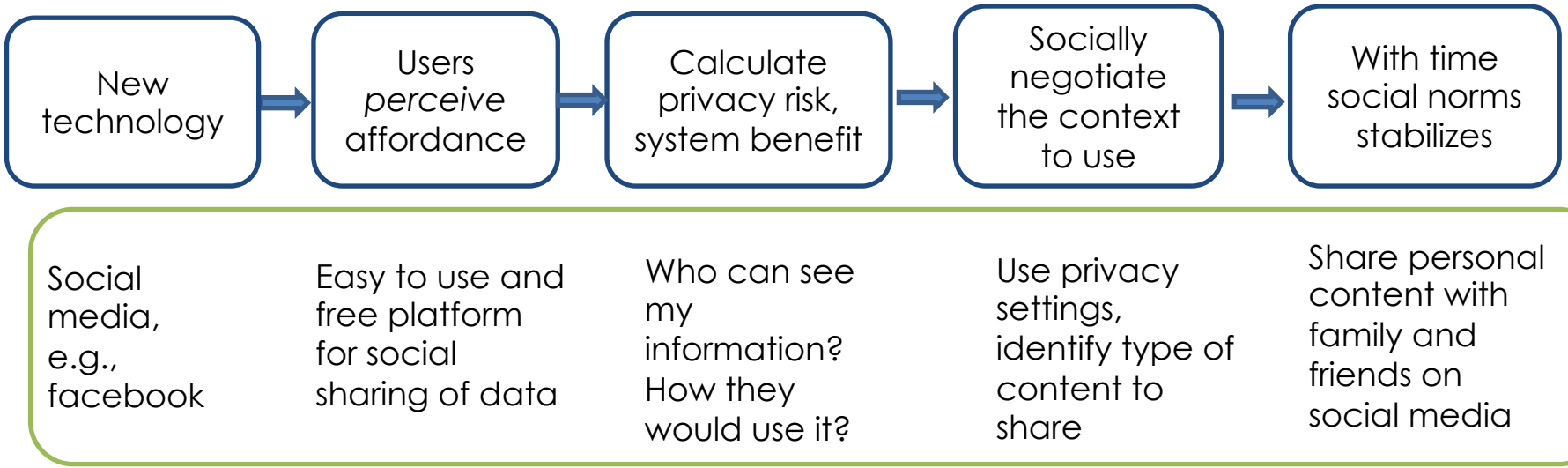
Social norms and privacy in systems



Don Norman 1988 and Gaver, CHI 1991

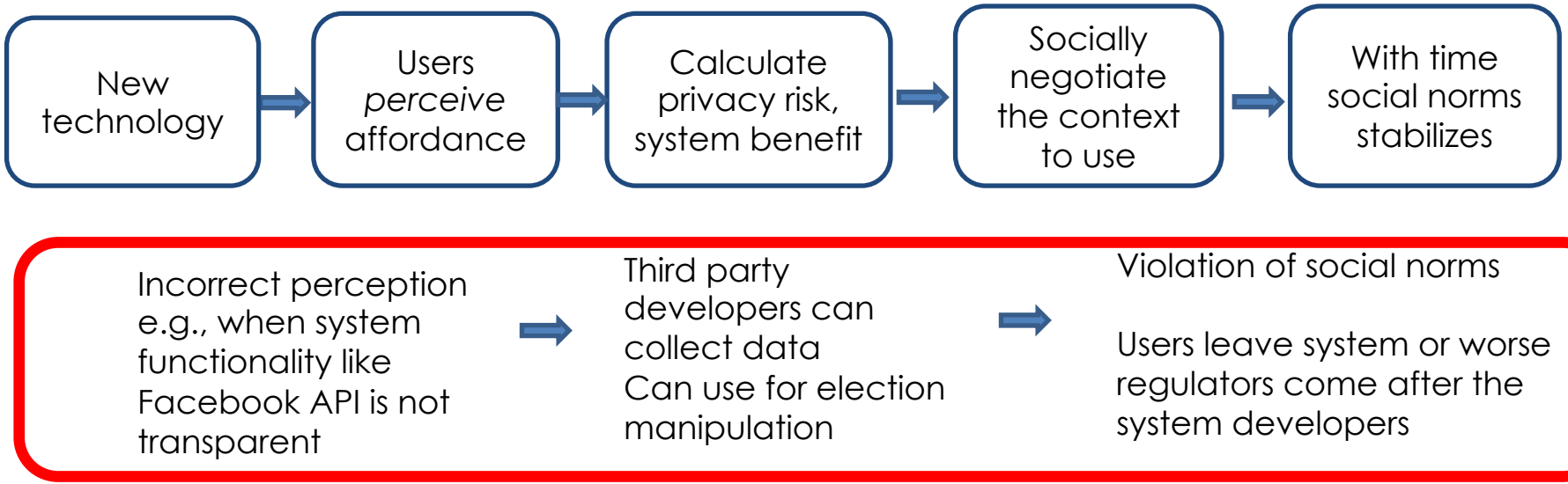
"The Development of Privacy Norms", Nicholas Proferes, 2022

Social norms and privacy in systems



Creation of social privacy norms

Social norms and privacy in systems



Violation of social privacy norms

New technologies violate social privacy norms

"*Each time when there was renewed interest in* ***protecting privacy*** *it was in* ***reaction to new technology***"

-- *Smith, 2004*

New technologies violate social privacy norms

"*Each time when there was renewed interest in* ***protecting privacy*** *it was in* ***reaction to new technology***"

-- *Smith, 2004*

There is a need for understanding social privacy norms for new technologies and social norm grounded system design

New technologies violate social privacy norms

"*Each time when there was renewed interest in* ***protecting privacy*** *it was in* ***reaction to new technology***"

-- *Smith, 2004*

There is a need for understanding social privacy norms for new technologies and social norm grounded system design

Social privacy norms are expressed by

- Shared mental models of a group of users
- Regulations or laws

Social norm grounded private system design

Social norm grounded private system design

Identify social norms given a particular context

+

Audit / build system to align with these norms

My research directions on aligning systems with social norms of security and privacy

Understanding the cultural norms of social disclosure

Understanding how social norms affect adoption of modern crypto wallets

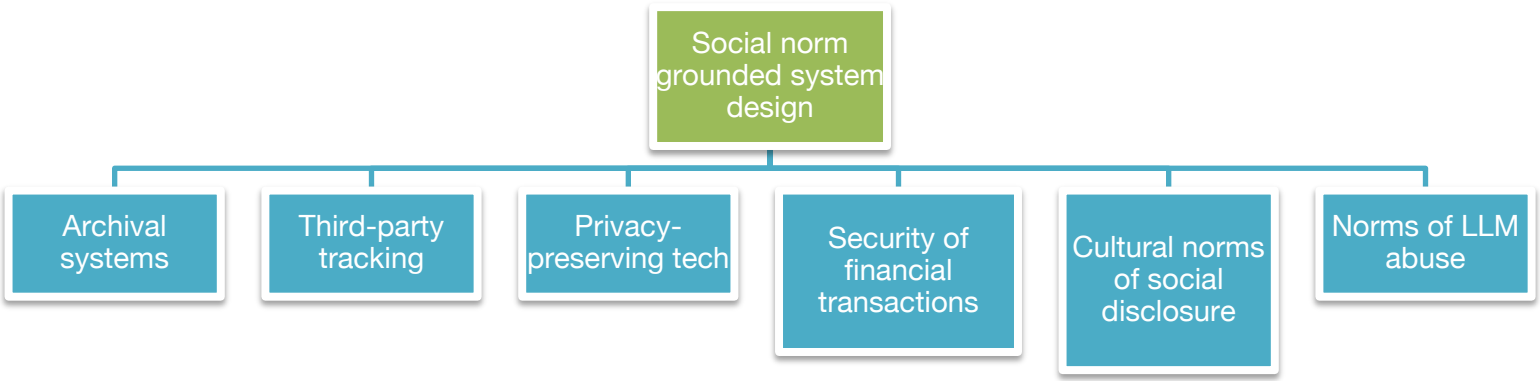
Overview of a few more threads of my research

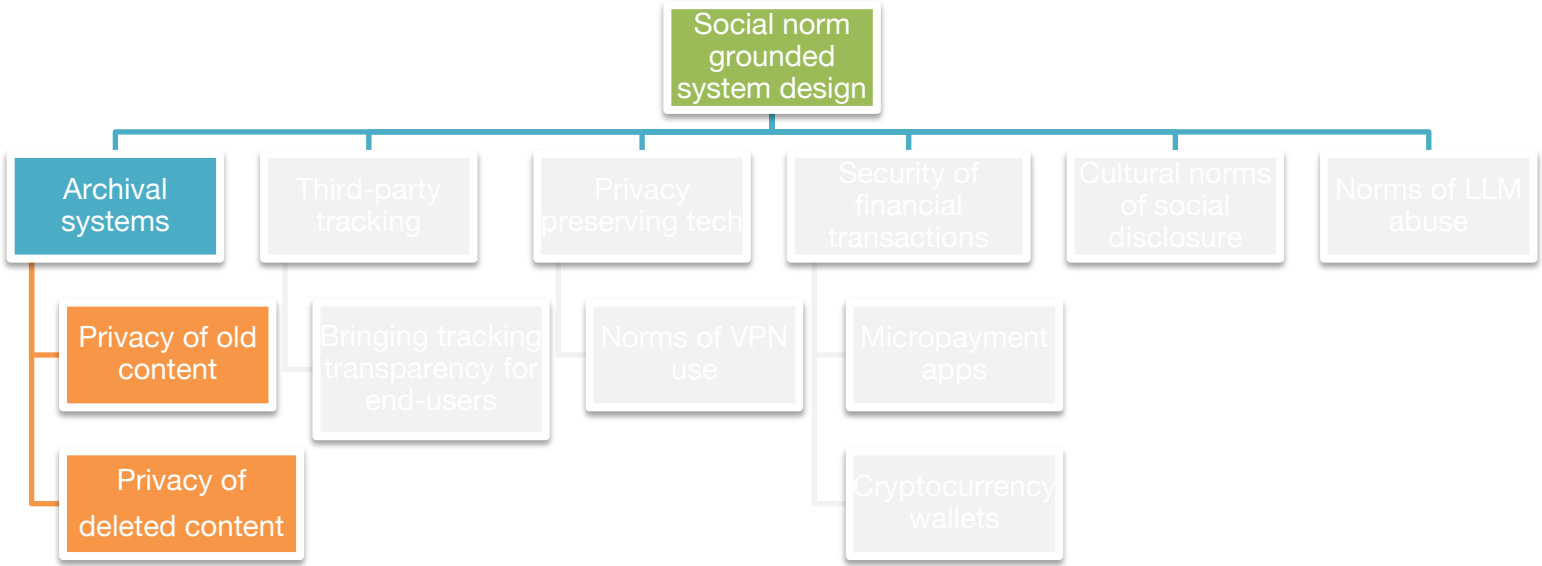
My research directions on aligning systems with social norms of security and privacy

Understanding the cultural norms of social disclosure

Understanding how social norms affect adoption of modern crypto wallets

Overview of a few more threads of my research


Social norm grounded system design
Archival systems
Third-party tracking
Privacy-preserving tech
Security of financial transactions
Cultural norms of social disclosure
Norms of LLM abuse



ASIACCS'23

Usenix Security 22 (2 papers)

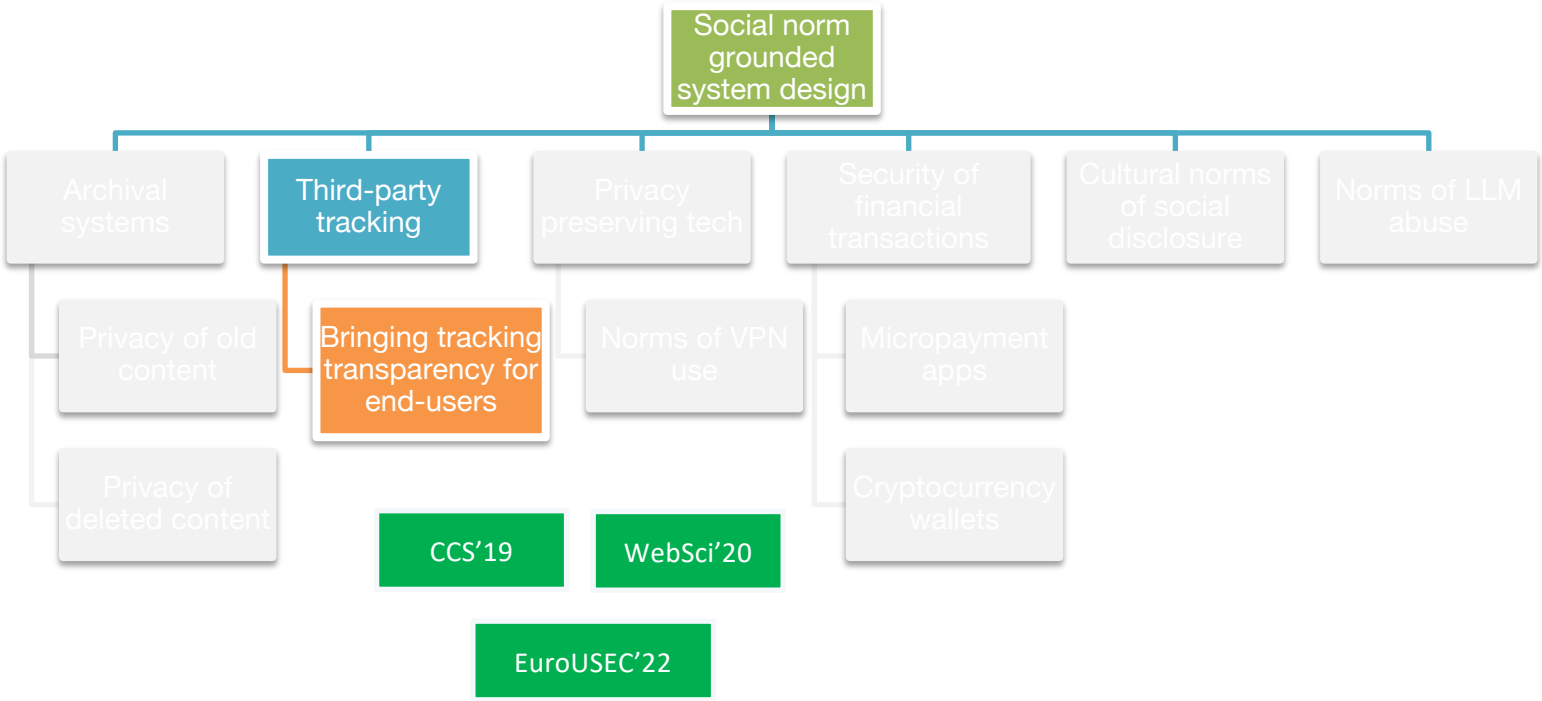
ICWSM'21

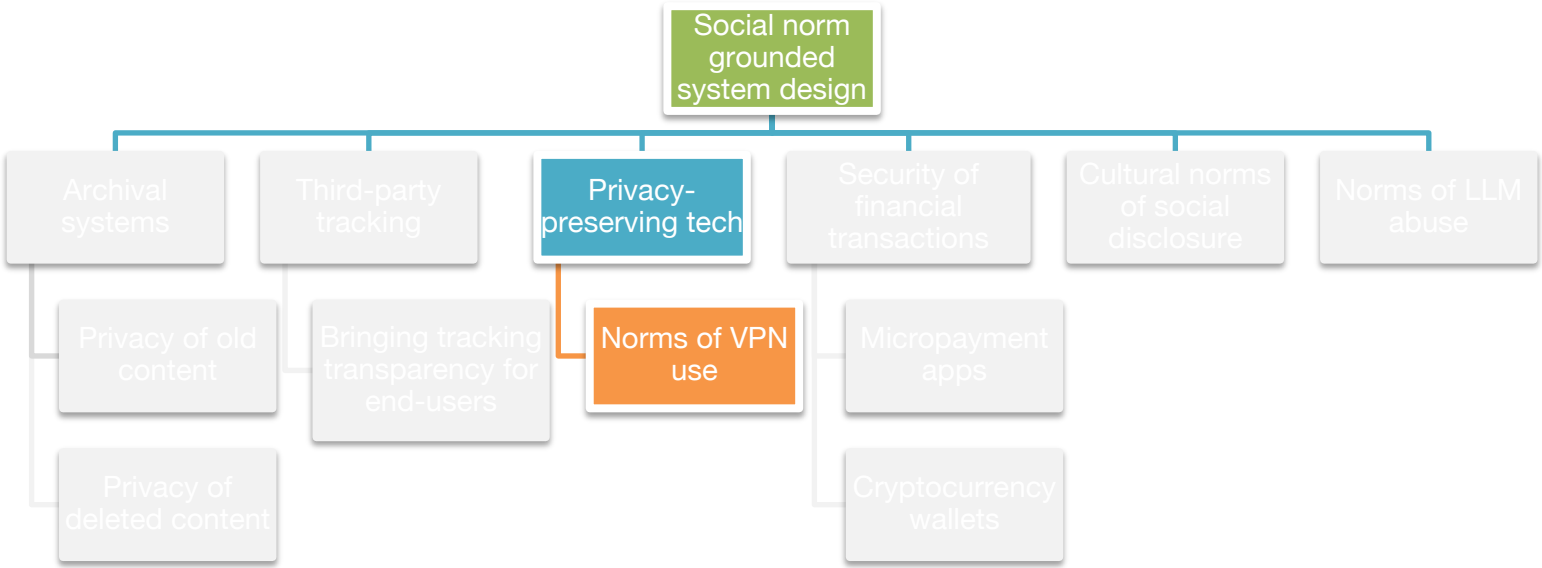
NDSS'21

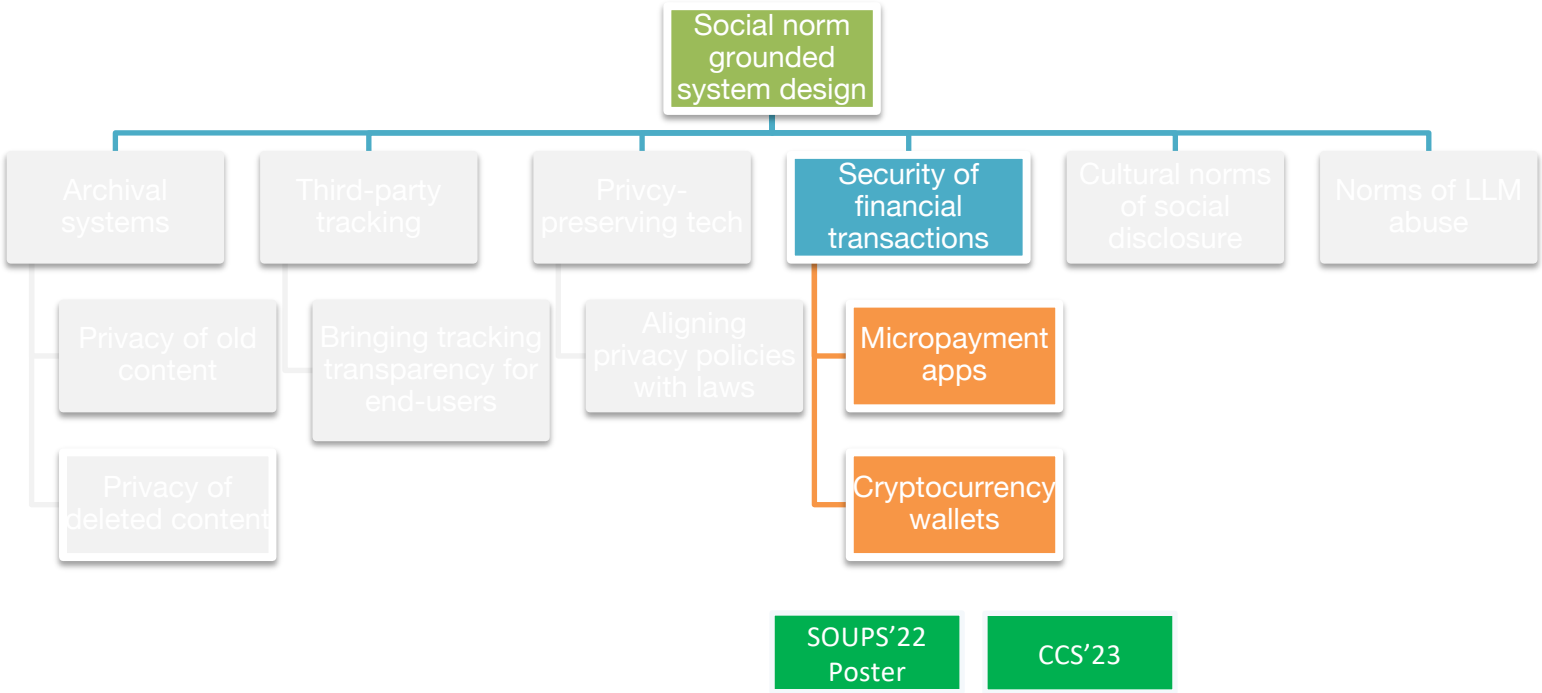
CCS'19

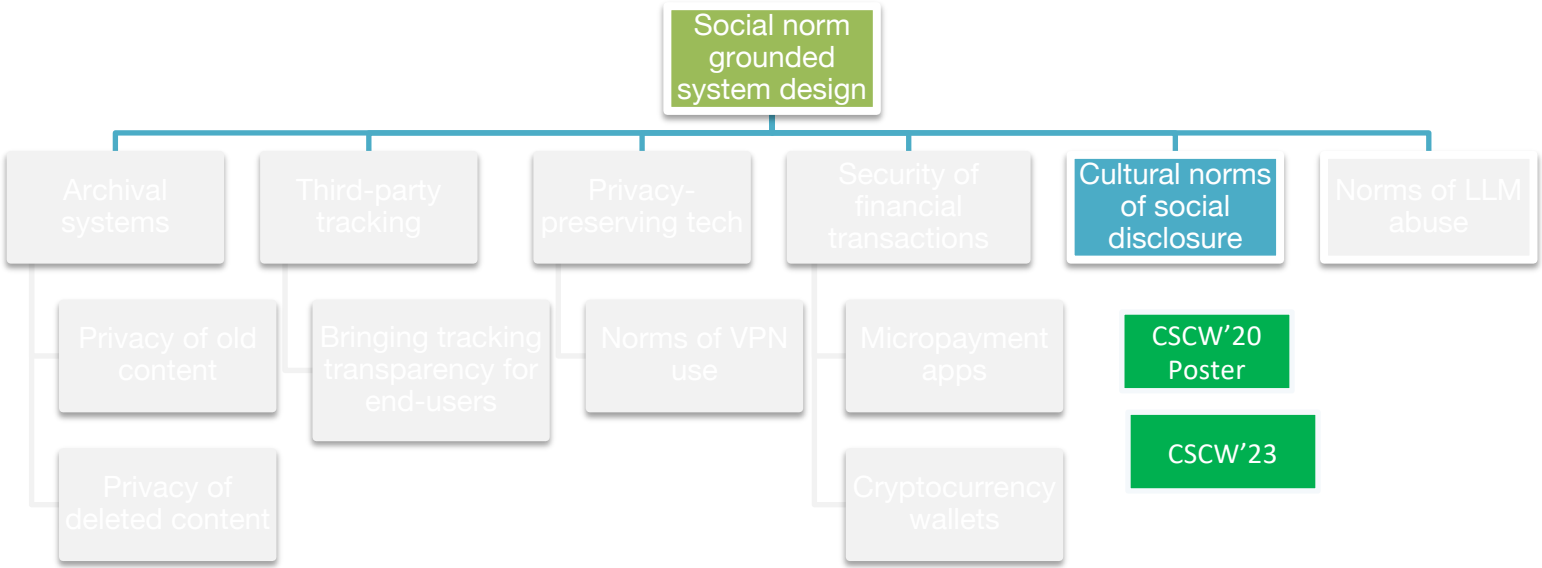
PETS'19

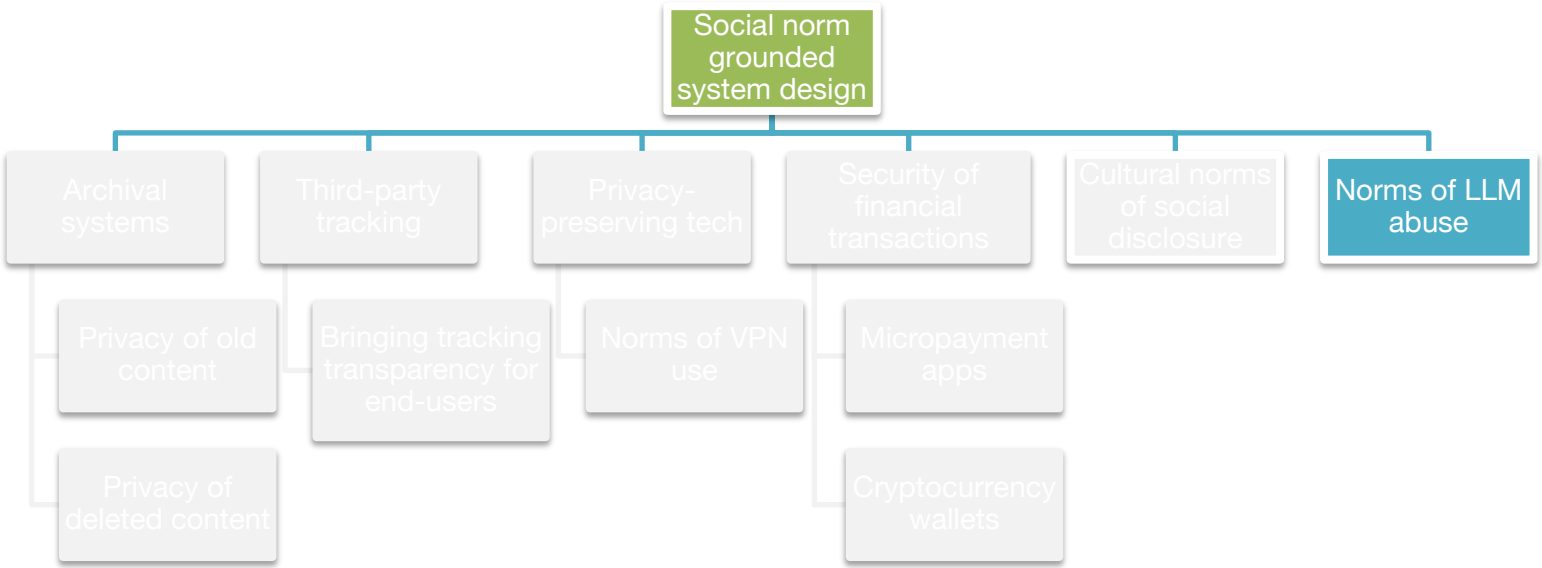
SOUPS'16

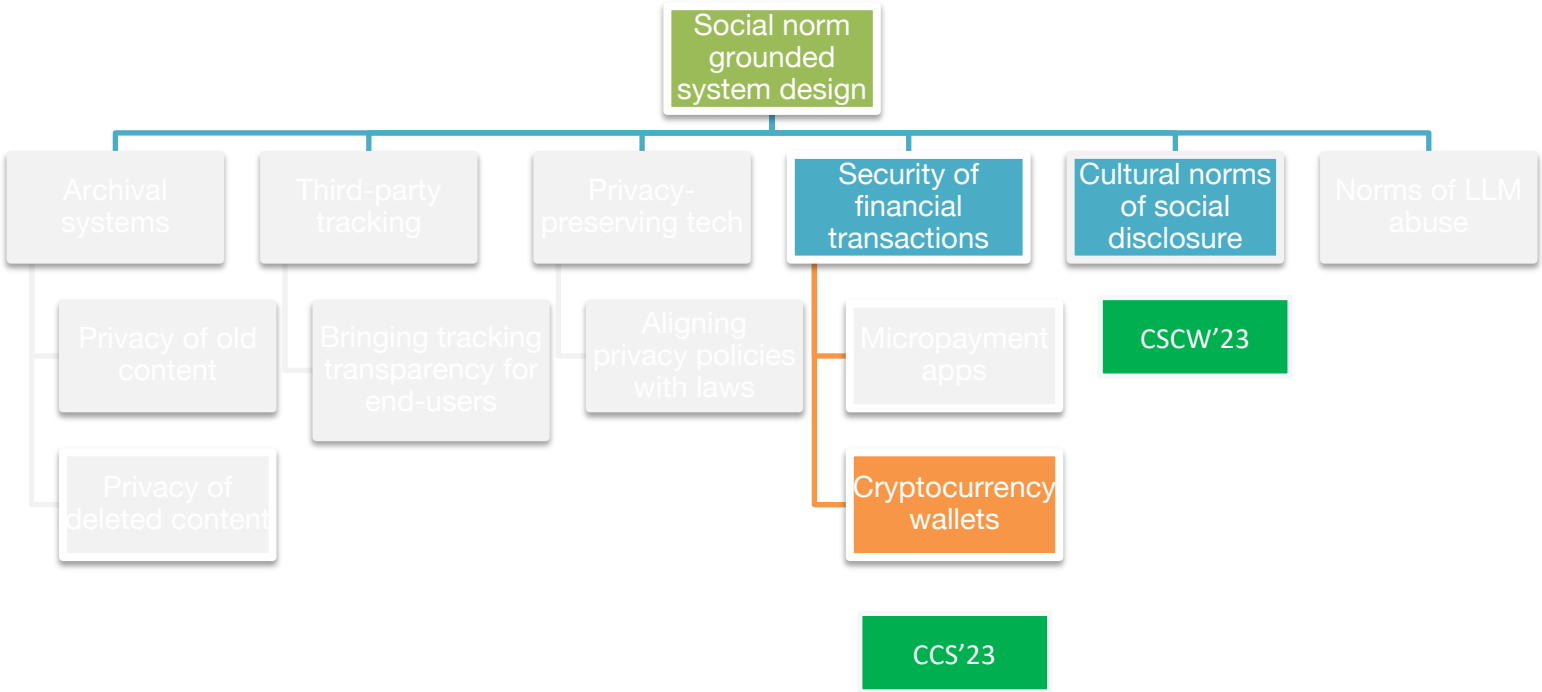

Social norm grounded system design
Archival systems
Third-party tracking
Privacy preserving tech
Security of financial transactions
Cultural norms of social disclosure
Norms of LLM abuse
Privacy of old content
Privacy of deleted content
Bringing tracking transparency for end-users
Norms of VPN use
Micropayment apps
Cryptocurrency wallets
CCS'19
WebSci'20
EuroUSEC'22


Social norm grounded system design
Archival systems
Third-party tracking
Privacy-preserving tech
Security of financial transactions
Cultural norms of social disclosure
Norms of LLM abuse
Privacy of old content
Privacy of deleted content
Bringing tracking transparency for end-users
Norms of VPN use
Micropayment apps
Cryptocurrency wallets


Social norm grounded system design
Archival systems
Third-party tracking
Privcy-preserving tech
Security of financial transactions
Cultural norms of social disclosure
Norms of LLM abuse
Privacy of old content
Privacy of deleted content
Bringing tracking transparency for end-users
Aligning privacy policies with laws
Micropayment apps
Cryptocurrency wallets
SOUPS'22 Poster
CCS'23


Social norm grounded system design
Archival systems
Third-party tracking
Privacy-preserving tech
Security of financial transactions
Cultural norms of social disclosure
Norms of LLM abuse
Privacy of old content
Privacy of deleted content
Bringing tracking transparency for end-users
Norms of VPN use
Micropayment apps
Cryptocurrency wallets
CSCW'20 Poster
CSCW'23


Social norm grounded system design
Archival systems
Third-party tracking
Privacy-preserving tech
Security of financial transactions
Cultural norms of social disclosure
Norms of LLM abuse
Privacy of old content
Privacy of deleted content
Bringing tracking transparency for end-users
Norms of VPN use
Micropayment apps
Cryptocurrency wallets


Social norm grounded system design
Archival systems
Third-party tracking
Privacy-preserving tech
Security of financial transactions
Cultural norms of social disclosure
Norms of LLM abuse
Privacy of old content
Privacy of deleted content
Bringing tracking transparency for end-users
Aligning privacy policies with laws
Micropayment apps
Cryptocurrency wallets
CSCW'23
CCS'23

My research directions on aligning systems with social norms of security and privacy

Archival systems | Third party tracking | VPN | Finance | Cultural disclosure | LLMs

Understanding the cultural norms of social disclosure

Understanding how social norms affect adoption of modern crypto wallets

Overview of a few more threads of my research

A Tale of Two Cultures

Comparing Interpersonal Information Disclosure Norms on Twitter

Photo of Holi Festival in Kolkata, India (left) by Dibakar Roy on Unsplash & Photo of times square, NYC, U.S. (right) by Vidar Nordli-Mathisen on Unsplash | Twitter logo from wikimedia commons

Mainack Mondal*, Anju Punuru*, Tyng-wen Scott Cheng+, Kenneth Vargas+, Chaz Gundry+, Nathan S Driggs+, Noah Schill+, Nathaniel Carlson+, Josh Bedwell+, Jaden Q Lorenc+, Isha Gosh**, Yao Li++, Nancy Fulda+, Xinru Page+

*IIT Kharagpur, India +Brigham Young University **University of Utah ++University of Central Florida

Social media allows people to connect across the globe

Social media **mediates disclosure** and social interactions which is key to **shaping interpersonal relationships**

Cultures shown to have different **offline disclosure norms** in terms of **emotion, topics, content shared**

Misinterpretation on social media causes friction, physical danger

Different cultural expectations could cause misunderstandings, hinder relationship formation, unintentional **conflict**

Multi-party privacy (MPP) especially problematic

When users disclose information **about someone else**

Multi-Party Privacy underexplored, especially **textual** content

Existing research focuses on norms of **Western** cultures

Cultural disclosure norms most often attributed to **collectivist verses individualist** dimension

Individualistic: independence, self-sufficiency, uniqueness
Collectivistic: Focus on group and social cooperation

We studied disclosure norms on Twitter

Compared **U.S.** and **India**

- Large user bases
- Western v. Asian culture
- English as common language (to facilitate comparison)

Public tweets collected Aug & Dec **2019**, Jan **2020**

Disclosures about their **interpersonal relationships**

Country	Users, in millions
United States	68.7
Japan	51.9
India	18.9
Brazil	16.65
Turkey	13.65
Indonesia	13.2
Saudi Arabia	12.35
Mexico	10.65
France	7.9
Canada	6.25
Germany	5.45

Overarching Research Question:

How do **interpersonal information disclosure norms** differ between **Indian** and **U.S.** tweets?

(a.k.a., what is typical to share about other people?)

Paper explores differences between India and U.S. for…

Frequency of disclosure about interpersonal relationships (family, friends, co-workers…)

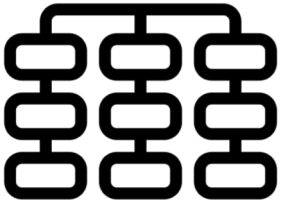
Topics of interpersonal information disclosures

Potentially sensitive information such as location and financial information

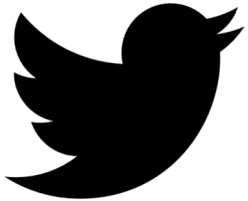
Frequency of various emotions disclosed

Frequency of positive/negative sentiment disclosed

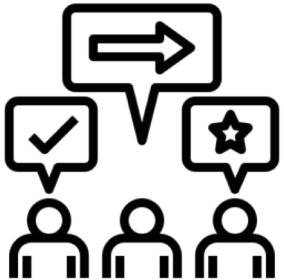
To study this we had to…



Create a culture-sensitive taxonomy of relationship words

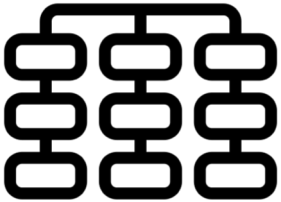


Collect tweets mentioning information about these relationships

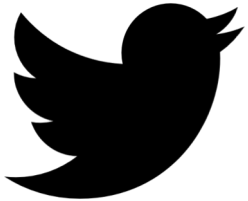


Identify culture specific norms for emotion, topic, and content

To study this we had to…



Create a culture-sensitive taxonomy of relationship words



Collect tweets mentioning information about these relationships

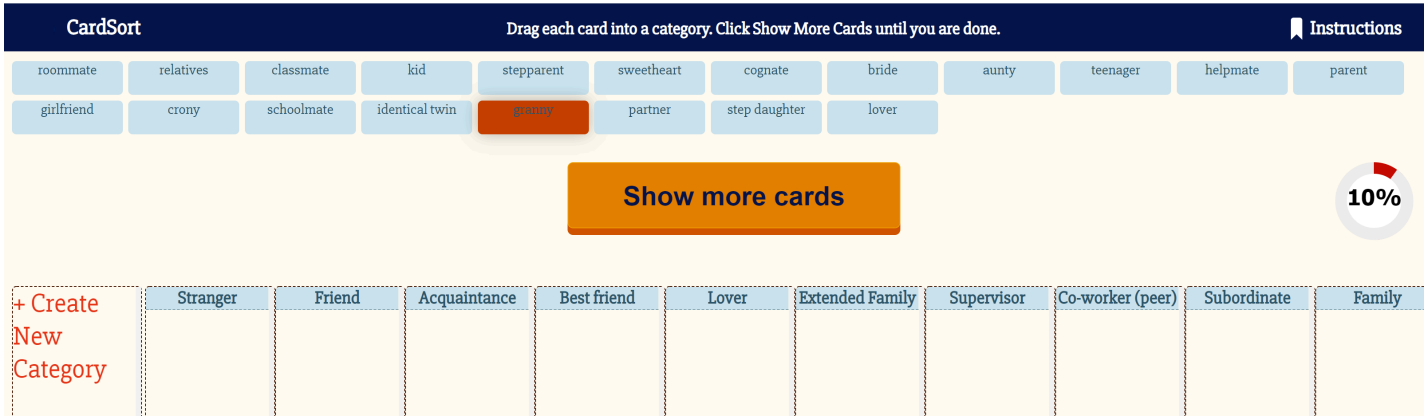
Identify culture specific norms for emotion, topic, and content

A hybrid card sort approach

3 U.S. and 2 India authors generated an initial **saturated list** of **relationship words** (177)

Had Mturk participants (58 Indian, 63 U.S.) sort relationship words into 10 categories based on **Relational model theory**

Ended up with **179 Indian** and **178 U.S. relationship words**



Final Culture-Specific Taxonomy

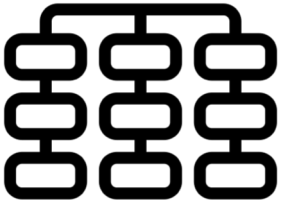
Words that consistently classified by **80% of participants in that culture** were included in taxonomy

	US	India
Uncle	**Extended Family**	**Family**
Wife, Husband	**Lover**	**Family**

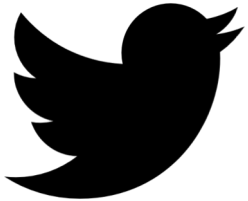
81 U.S. words
112 India words
9 relationship categories

Supervisor	India	advisor, boss, guru, manager, master, mentor, seni
	U.S.	advisor, boss, guru, manager, master, mentor, seni
Co-worker	India	cohort, colleague, coworker, co-worker, helpmate,
	U.S.	associate, colleague, coworker, co-worker, teamma
Subordinate	India	associate, junior, mentee, subordinate
	U.S.	mentee, subordinate
Friend	India	bosom buddy, bro, buddy, chum, classmate, friend, f
		roommate, schoolmate

To study this we had to…



Create a culture-sensitive taxonomy of relationship words



Collect tweets mentioning information about these relationships

Identify culture specific norms for emotion, topic, and content

Collecting initial set of tweets

Twint used to collect historical English tweets from India and U.S. containing **relationship words**

Random sample of tweets

Representative in terms of time and popularity

~2 million U.S. tweets **~272K Indian** tweets

Public tweets Aug & Dec **2019**, Jan **2020**

Identifying personal relationships

Need to filter down to tweets about the **poster's personal relationships**

Personal:
My **daughter's** health has been one of my biggest worries. She was a premature baby

Not:
Kobe and his **daughter**. May they rest in peace forever! My next jump shot is for her

Developing a dependency-parsing based classifier

Possessive tuples: Words indicating relationships (**me, my, our**)

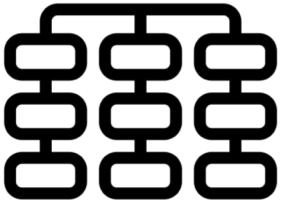
Idea: Relationship word should have dependency with a word in possessive tuple

Dependency parsing to create a novel classifier

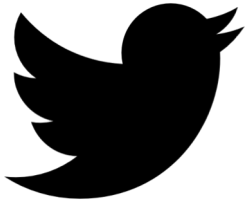
Evaluated using manually coded ground truth
86% F1-Score , 92% Precision, 81% Recall

Final dataset of **417,953 U.S**. Tweets and **33,591 Indian** tweets

To study this we had to…



Create a culture-sensitive taxonomy of relationship words



Collect tweets mentioning information about these relationships

Identify culture specific norms for emotion, topic, and content

Paper explores differences between India and U.S. for…

Frequency of disclosure about interpersonal relationships (family, friends, co-workers…)

Topics of interpersonal information disclosures

Potentially sensitive information such as location and financial information

Frequency of various emotions disclosed

Frequency of positive/negative sentiment disclosed

Paper explores differences between India and U.S. for…

Frequency of disclosure about interpersonal relationships (family, friends, co-workers…)

Topics of interpersonal information disclosures

Potentially sensitive information such as location and financial information

Frequency of various emotions disclosed

Frequency of positive/negative sentiment disclosed

Topics of interpersonal disclosure

LDA and thematic analysis to identify topics of disclosure

U.S.		India	
Topics Disclosed	% Tweets	Topics Disclosed	% Tweets
Stories about Family	35.5%	Stories about Family	26.1%
Complaining	10.6%	Celebrations	25.9%
Gratitude	10.4%	Expressing Love	19.5%
Celebrations	9.8%	Patriotism	9.7%
Christianity	8.9%	Work	5.7%
Politics	6.8%	Schooling	4.7%
Profane Narrative	5.9%	Reminiscing	3.4%
Female Romantic partner	5.0%	Complaining	2.9%
Schooling	3.8%	Other	2.0%
Social Media Activities	1.6%		
Work	0.9%		
Reminiscing	0.8%		

How do the disclosed topics differ?

Common	US	India
Stories about Family, Complaining, Celebrations, Reminiscing	Gratitude, **Politics**, Female Romantic partner, Profane Narrative	**Patriotism**, Expressing Love

U.S. tweets mention **politics** while talking about family
vs.
Indian tweets express **patriotism** when talking about family/kids

Even common topics are not the same

Common	US	India
Stories about Family, **Complaining**, Celebrations, Reminiscing	Gratitude, Politics, Female Romantic partner, Profane Narrative	Patriotism, Expressing Love

U.S. tweets **complain** about family members
vs.
Indian tweets **complain** about organizations

“Glad to grow with my beloved aunt”
(India)

vs.

“my f*****g aunt p**sed me off”
(US)

Some take aways

Collectivist cultures focus on **in-group harmony** => more **positive** tweets

Must study Supervisor-Subordinate relationships, less studied offline.
e.g., Collectivist emphasizes **hierarchical status and social order** vs. more **positive** tweets about U.S. **subordinate**

Acceptable topics will differ
India => No complaints about family, self-promotion
U.S. => profanity and angry political complaints

Check paper to know more

My research directions on aligning systems with social norms of security and privacy

- Archival systems
- Third party tracking
- VPN
- Finance
- Cultural disclosure
- LLMs

Understanding the cultural norms of social disclosure

- US and India differs in terms of what to share about their social relationships

Understanding how social norms affect adoption of modern crypto wallets

Overview of a few more threads of my research

My research directions on aligning systems with social norms of security and privacy

Archival systems

Third party tracking

VPN

Finance

Cultural disclosure

LLMs

Understanding the cultural norms of social disclosure

US and India differs in terms of what to share about their social relationships

Understanding how social norms affect adoption of modern crypto wallets

Overview of a few more threads of my research

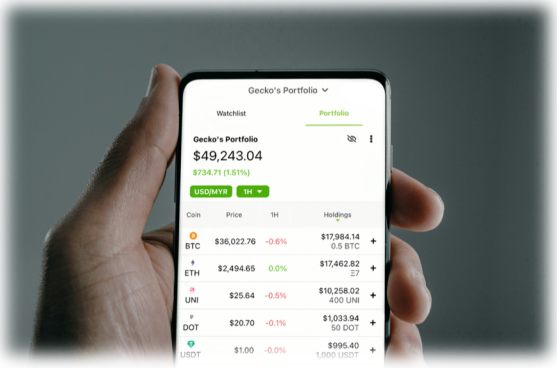
Uncovering Impact of Mental Models towards Adoption of Multi-device Wallets

Easwar Vivek Mangipudi [+], Udit Desai*, Mohsen Minaei [+], Mainack Mondal*, Aniket Kate [+]

[+] Purdue University *IIT Kharagpur

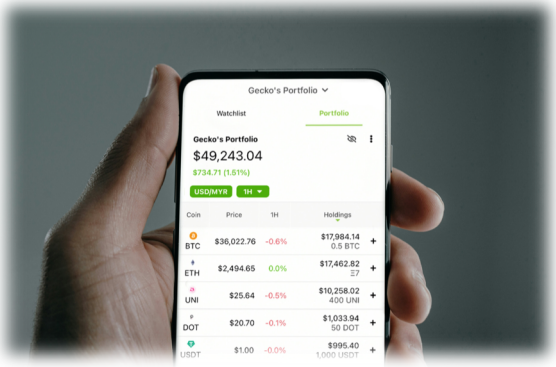
Cryptocurrency userbase in growing

- Rapid increase in Cryptocurrency users
  - Users - 430 million 2023
  - Market size - $10.27 billion in 2023
    - Estimated to reach $48.27 billion by 2030



Cryptocurrency userbase in growing

- Rapid increase in Cryptocurrency users
  - Users - 430 million 2023
  - Market size - $10.27 billion in 2023
    - Estimated to reach $48.27 billion by 2030



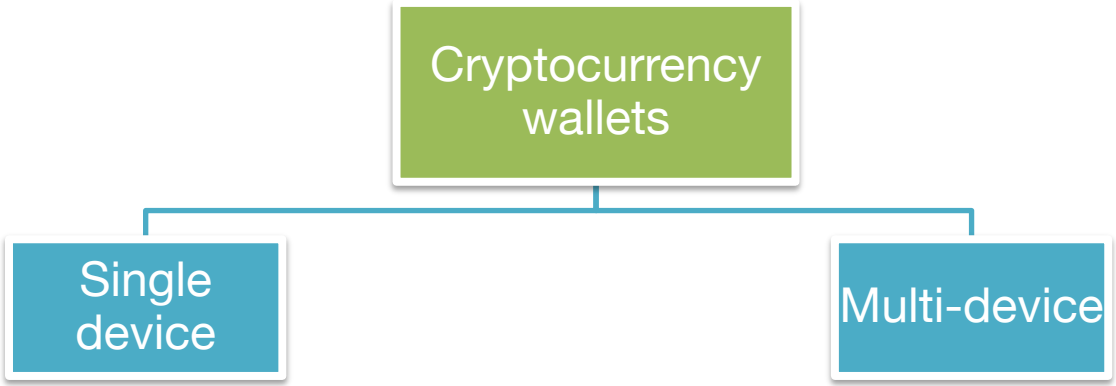
- Users need cryptocurrency wallets for storing and trading their cryptocurrency

Cryptocurrency Wallets

Every crypto currency wallet is associated with a secret key - public key pair

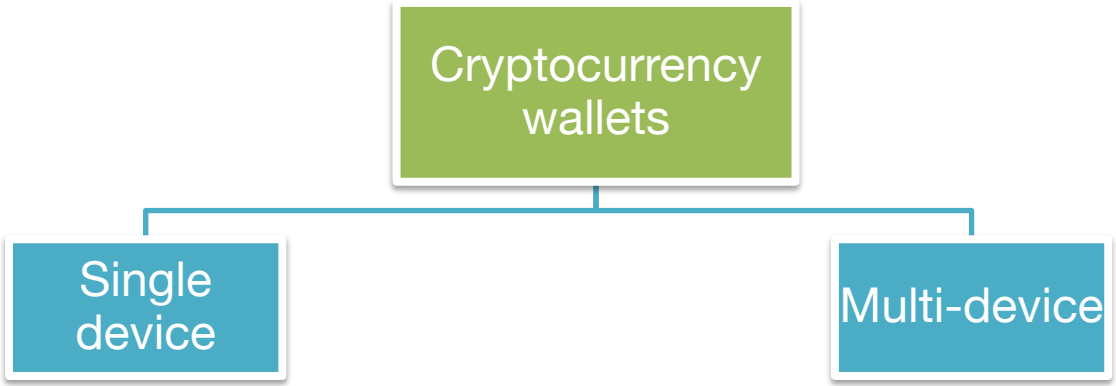
Cryptocurrency Wallets

Every crypto currency wallet is associated with a secret key - public key pair



Cryptocurrency Wallets

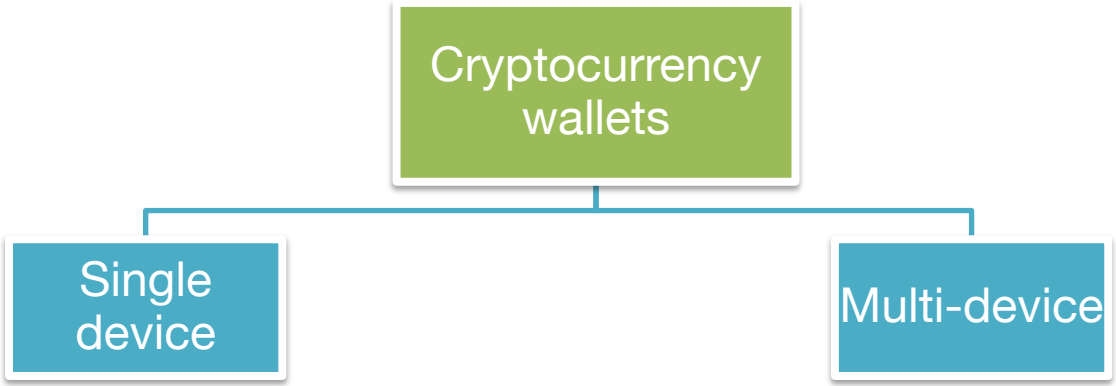
Every crypto currency wallet is associated with a secret key - public key pair



secret key is stored on a single device: Phone, laptop, hardware-key, brain, paper

Cryptocurrency Wallets

Every crypto currency wallet is associated with a secret key - public key pair



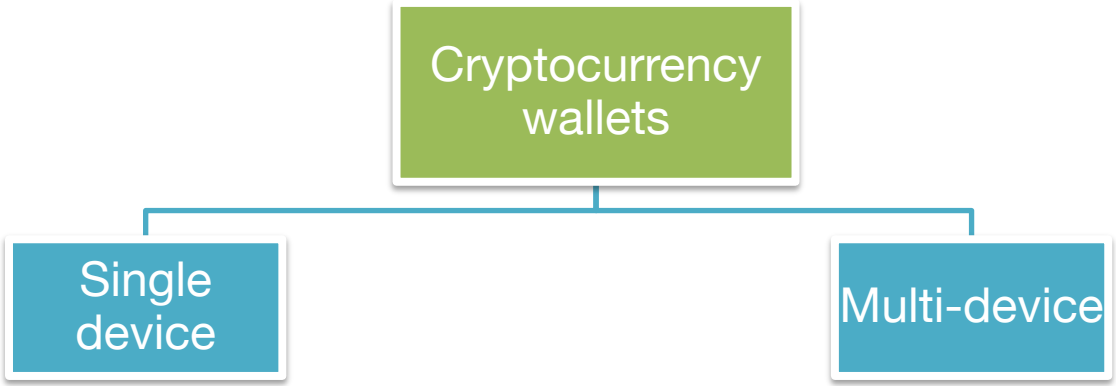
secret key is stored on a single device: Phone, laptop, hardware-key, brain, paper

Secret key is distributed among multiple devices: user devices or different servers, can belong to the same user/company or multiple

Multi-sig or threshold

Cryptocurrency Wallets

Every crypto currency wallet is associated with a secret key - public key pair



secret key is stored on a single device: Phone, laptop, hardware-key, brain, paper

Secret key is distributed among multiple devices: user devices or different servers, can belong to the same user/company or multiple

Multi-sig or threshold

Single and Multi-device differs in terms of security guarantees

Attacks on Cryptocurrency Wallets

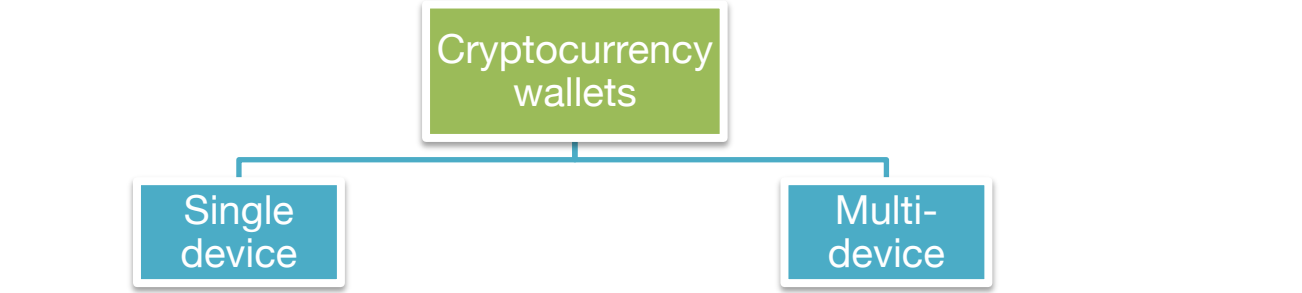
~20% of all bitcoins stolen

- $2.6 billion stolen from cryptocurrency exchanges since 2012
- Total crypto hacks value much more

Attacks on Cryptocurrency Wallets

~20% of all bitcoins stolen

$2.6 billion stolen from cryptocurrency exchanges since 2012
Total crypto hacks value much more



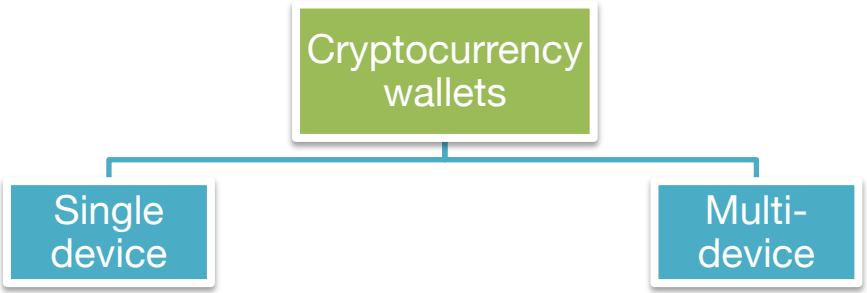
more vulnerable to loss or compromise of keys
No key recovery

less vulnerable
Adversary needs to compromise multiple machines

Attacks on Cryptocurrency Wallets

~20% of all bitcoins stolen

$2.6 billion stolen from cryptocurrency exchanges since 2012
Total crypto hacks value much more



more vulnerable to loss or compromise of keys
No key recovery

less vulnerable
Adversary needs to compromise multiple machines

Still single device wallets seems to be more popular. **Why?**

Research Questions

- RQ1: What are the current preferences of cryptocurrency wallets?
- RQ2: Provided essential information regarding different wallets are given, the users willing to shift to multi-device wallets?
- RQ3: What default key-management and architectural settings do they prefer for different wallets?

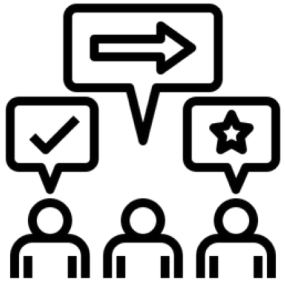
Research Questions

- RQ1: What are the current preferences of cryptocurrency wallets?
- RQ2: Provided essential information regarding different wallets are given, the users willing to shift to multi-device wallets?
- RQ3: What default key-management and architectural settings do they prefer for different wallets?

Study design

General questions about cryptocurrency wallet usage and preferences

Educate using showing two videos and a short knowledge-test



Questions to check preferences and perceptions regarding cryptocurrency wallets

Recruitment

- Recruitment from Prolific academic
  - Total 357 form US, UK, Canada
  - Male - 70.5%, Female 27.7%
  - 62.7% have Bachelor's or higher degree
  - 72.2% are full time employees

- Median time - 22 minutes

Research Questions

- RQ1: What are the current preferences of cryptocurrency wallets?
- RQ2: Provided essential information regarding different wallets are given, the users willing to shift to multi-device wallets?

RQ1: Existing preferences

- Two user groups emerged
  - Newbies: Started for the fear of missing out (86 users)
  - Non-newbies: Primary venue of trade, interest in technology (271 users)
  - Statistically different #years of usage, experience, knowledge

RQ1: Existing preferences

- Two user groups emerged
  - Newbies: Started for the fear of missing out (86 users)
  - Non-newbies: Primary venue of trade, interest in technology (271 users)
  - Statistically different #years of usage, experience, knowledge
- Both groups mostly use single-device wallets
  - Coinbase (66%), Metamask and Binance (39%)
  - **~50% "Not familiar"** with multi-device wallets

Research Questions

- RQ1: What are the current preferences of cryptocurrency wallets?
- RQ2: Provided essential information regarding different wallets are given, the users willing to shift to multi-device wallets?

RQ2: Preferences after watching video

- Around 40% of newbies/non-newbies are still not-willing to shift from single-device to multi-device
  - 51% *told* they would shift

RQ2: Preferences after watching video

- Around 40% of newbies/non-newbies are still not-willing to shift from single-device to multi-device
  - 51% *told* they would shift

	Reasons	%
Not willing	Single-device wallets are more secure	38.8%
	Single-device wallets are simple to use	24.8%
	I do not want to lose control of keys	15.6%
	Other reasons	19.8%
Willing	Multi-device wallets are more secure	79.7%
	Other reasons including availability	20.29%

RQ2: Preferences after watching video

- Around 40% of newbies/non-newbies are still not-willing to shift from single-device to multi-device
  - 51% *told* they would shift

	Reasons	%
Not willing	Single-device wallets are more secure	38.8%
	Single-device wallets are simple to use	24.8%
	I do not want to lose control of keys	15.6%
	Other reasons	19.8%
Willing	Multi-device wallets are more secure	79.7%
	Other reasons including availability	20.29%

What is their rationale?

"I like to keep things simple, easy to access and without complexities" – P57

"I prefer to be responsible for my keys. If I lose them, that is my fault" – P1

What is their rationale?

"I like to keep things simple, easy to access and without complexities" – P57

"I prefer to be responsible for my keys. If I lose them, that is my fault" – P1

"I am happy to be in control of the key as I believe the risk is low" – P51

"I prefer the single storage location. One location is easier to secure than multiple ones" – P107

What is their rationale?

"I like to keep things simple, easy to access and without complexities" – P57

"I prefer to be responsible for my keys. If I lose them, that is my fault" – P1

*"I am happy to be in control of the key as **I believe the risk is low**" – P51*

*"I prefer the single storage location. **One location is easier to secure than multiple ones**" – P107*

Summary

- Multi-device wallets have low adoption
  - Wrong mental model about security of wallets
- Need to nudge and educate users
  - Customization for two user-groups newbies and non-newbies
- Novel cryptographic schemes needed
  - Greater weightage to client devices than a server hosting the key
  - Resonates with NIST's call for secure threshold cryptographic protocols that maintains the users' control over the keys

My research directions on aligning systems with social norms of security and privacy

- Archival systems
- Third party tracking
- VPN
- Finance
- Cultural disclosure
- LLMs

Understanding the cultural norms of social disclosure

- US and India differs in terms of what to share about their social relationships

Understanding how social norms affect adoption of modern crypto wallets

- Users need more agency over keys to make crypto-wallets usable

Overview of a few more threads of my research

My research directions on aligning systems with social norms of security and privacy

- Archival systems
- Third party tracking
- VPN
- Finance
- Cultural disclosure
- LLMs

Understanding the cultural norms of social disclosure

- US and India differs in terms of what to share about their social relationships

Understanding how social norms affect adoption of modern crypto wallets

- Users need more agency over keys to make crypto-wallets usable

Overview of a few more threads of my research

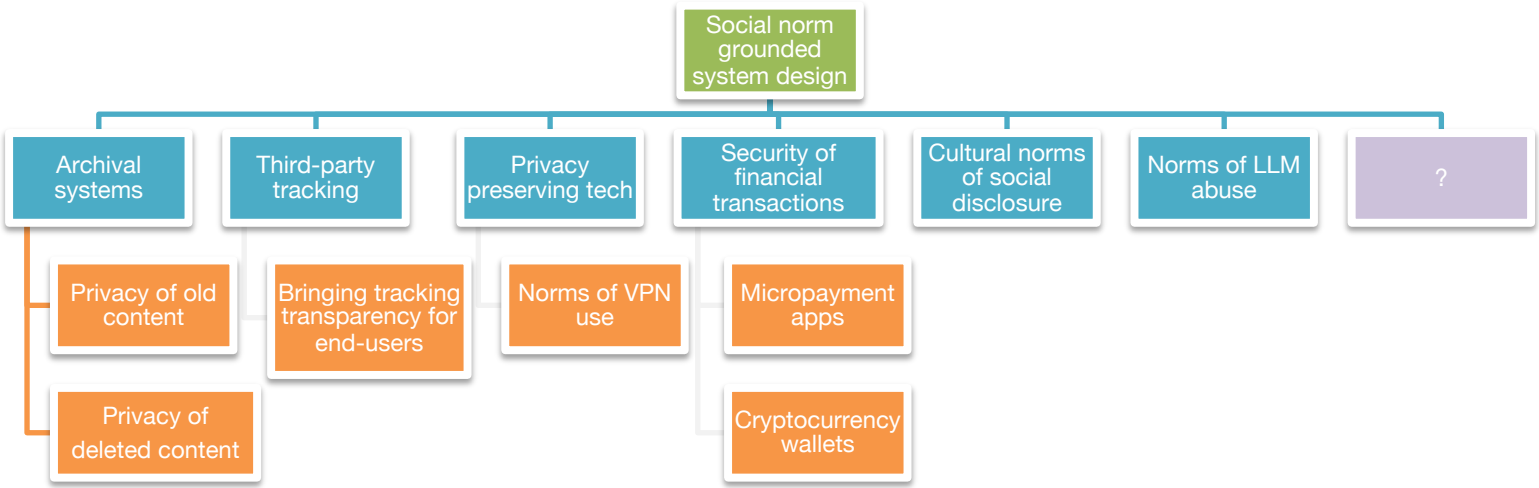
A few other research directions

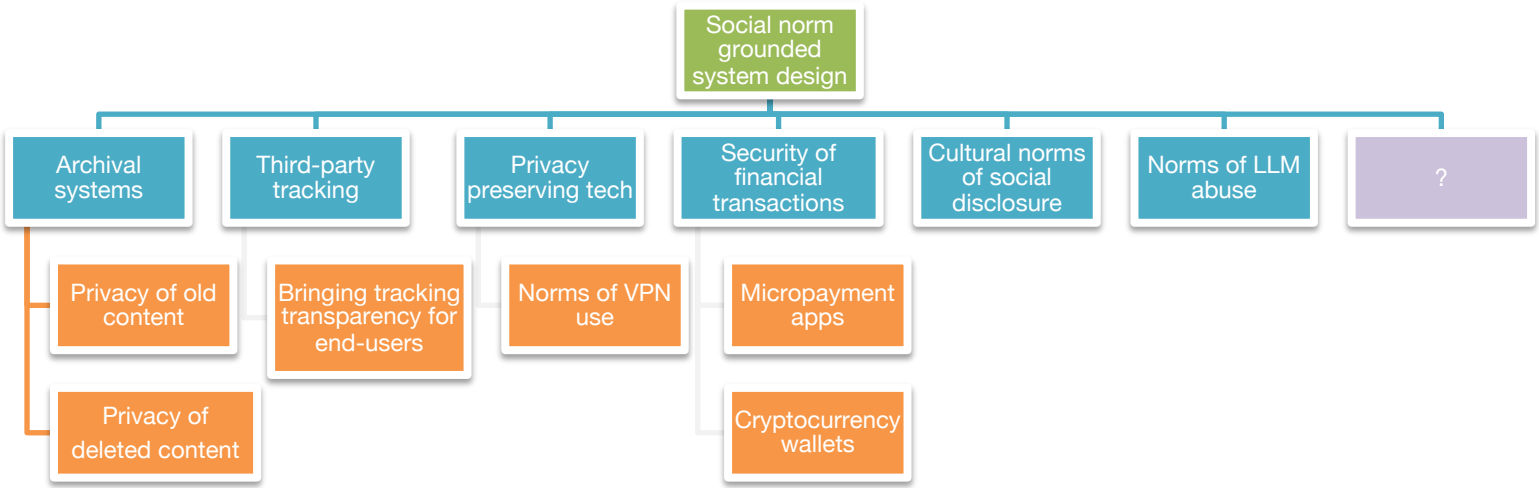
Combating online manipulation

- Combating Hatespeech
- Combating Covid-19 misinformation
- Detecting and combating logical fallacies in online discouse

Privacy education

- Creating visual intervention for Facebook users to educate about advertising
- Educating users to combat domestic partner surveilance


Social norm grounded system design
Archival systems
Third-party tracking
Privacy preserving tech
Security of financial transactions
Cultural norms of social disclosure
Norms of LLM abuse
?
Privacy of old content
Privacy of deleted content
Bringing tracking transparency for end-users
Norms of VPN use
Micropayment apps
Cryptocurrency wallets



https://cse.iitkgp.ac.in/~mainack/

mainack@cse.iitkgp.ac.in