CS-234
Technologies for Democratic society

Fall 2021

Week 13

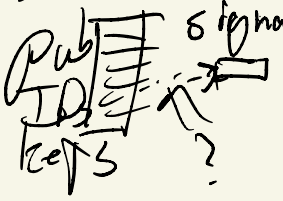
Anonymous identity cover (cont'd)

Pseudonymization techniques
- Randomized Mac addresses
- 4chan tags, public keys, Blockchain wallets

weakness: linkable over time

Stronger: Ephemeral pseudonyms (eg. 1-use)
: Mixing (Bitcoin, Monero)
: Zero-knowledge proofs (Zcash)

Anonymous credentials
Attestor → "over 18" cred → randomization → show + bar
group/ring signature



Accountable anonymous identity

- threshold of approval
- traceability: authority can revoke anonymity
- 1-to-1 mappings of IDs/keys to pseudonyms
  - linkable ring signatures
  - 1-of-1 pseudonymized credentials;
    - Crypto-Book - social media creds
    - CanDID - using govt ID, AVS#
- Blacklistable anonymous credentials

Polarization

- we have an existing, self-selected "circle"
  we get most influence from them
  common existing biases → reinforced
  non-conforming opinions → suppressed, excluded
- related: "groupthink"

Polarization online

- self selecting friend/follow communities
  newsfeeds reinforce existing biases →
  polarization, radicalization
- recommendation systems (Youtube)
  - reinforcing local social neighborhood perspectives
  - eyeball time maximizing algorithms
    learns from user behavior
    emotional content → more viewing
  - only more extreme content "stands out"
  - shocking news gets circulated more/faster

Mitigating polarization/radicalization

- Broader newsfeeds (does it work?)
- social connection/interaction w/ those holding other viewpoints
- reducing sense of "anonymity" - lack of pressure for civility
- Labeling information