Collaborative Access

- A content pertains to multiple owners
- Group photo: A person "owns" it but those in the picture should have a right to claim privacy (i.e., co-owners)
- How to decide who is a co-owner?
- Ex: Alice shares a picture with Bob. Alice wants all her friends to see but Bob does not want Charlie to see it.
- Which policy to apply?
Mechanisms to enable collaborative access

- Possible incentives for collaboration
  - Credit system so that users can later use this to claim their own privacy; e.g., Squicciarini *et al.*
  - Employ social norms; e.g. reciprocity
  - Alternatives?

- Dealing with multiple policies
  - Selective disclosure (e.g., blur a person? Faceblock http://face-block.me/)
  - Select one policy among all (Squicciarini *et al.*)
  - Collaborate to create one policy (Wishart *et al.*)
  - Find a middle ground (e.g., negotiate) among policies
Squicciarini et al. use Clarke-Tax approach

- Each user has a policy and a valuation for that policy
- When the user is a co-owner, she can place a bid
- The bid value is bound by the credits allocated in the system
- The policy yielding highest social welfare is chosen and the users that contribute gets taxed
- Alternatives? Highest bid? Minimum common ground?

Example
Co-authoring Policies

- Content owner
  - Creates a privacy policy for the content she wants to put up.
  - Shares the privacy policy with those relevant (e.g., tagged) so that they (co-owners) can modify it.
- A privacy policy states a set of permitted actions on a resource
- Strong conditions can be added by all
- Weak conditions can be added or modified or deleted
Example Policy (Wishart et al.)

```
policy p{
    strong-conditions:
        request_by(Y),
        group('Alice', Y, 'Family')
    weak-conditions:
        not friend_in_touch('Bob', 'Y')
resource: 'Birthday party'
can-do: view
}
```

Birthday party pictures can be viewed by Alice’s family and not by those that are in touch with Bob.
Policy Evaluation

- D: Translated into a set of Datalog rules of the form $A \land B \ldots \implies H$, where the head (H) corresponds to the permission
- B: Domain rules
- R: Relations
- $perm(t, q)$: Action t is permitted for query q
- Permit if $D \cup B \cup R \models perm(t, q)$
What is wrong with users’ editing a policy jointly?
- Privacy
- Ease of use
- Consistency

Alternatives?
- Possible to reach an agreement without disclosing privacy policies?
- Possible to automate the process so the users are minimally involved?
