Communal Sharing of Sensitive Data

Internatioal Data Week – SciDataCon 2018
Gaborone, Botswana

Tyng-Ruey Chuang and Chih-hsing Ho
Academia Sinica
Taipei, Taiwan

trc@iis.sinica.edu.tw
chihho@gate.sinica.edu.tw

Outline

- Privacy and the Use of Personal Data
- Communal Sharing of Resources
- Sharing Sensitive Information
- Social Media, Federations, and Coop Platforms

Privacy

- “The right to be let alone”
- Properties attributed to an individual
- Personal identifiable information

- Often referring not merely restrictions on acquiring personal data, but a set of principles and rules that govern the use of personal information and its disclosure.

Critics on the Current Practices

- Individual privacy, aggregation of data, group profiling.
- Three kinds of actors: **individuals** in a population from whom data is collected; **data controllers** who get hold of the data and decide on how it is used; various **third parties** who want access to the data.
- A central dilemma: Individuals, controllers, and third-party data users do not have their interests properly aligned when sharing and reusing personal data.

- The usual ways: informed consent, de-identification, etc.
- Problems: re-identification, benefit distribution, etc.

Project Goals

- To survey and develop the governing principles of a communal approach to personal data management where the members of a community pool sensitive information about themselves for mutual benefits.
- To develop and put into use the methods, tools, and information systems to facilitate communal sharing of sensitive data.

- Work in progress!

A Communal Approach: Some Analogies

- Collaborative data collection and aggregation
  - OpenStreetMap
- Benefit sharing without centralization
  - GPL license (for copylefted software, e.g. Linux)
- Management of common-pool resources
  - Works by Elinor Ostrom
  - Irrigation systems, forests, etc. – neither state nor market
- Issues:
  - mechanisms to incentivize sharing, ways for fair distribution of benefits, methods to enforce group boundary, and workable procedures to form censuses and decisions, etc.

Elinor Ostrom: Design Principles of Common-pool Resource Institution

- *Clearly defined boundaries should be in place.*
- *Rules in use are well matched to local needs and conditions.*
- *Individuals affected by these rules can usually participate in modifying the rules.*
- *The right of community members to devise their own rules is respected by external authorities.*
- *A system for self-monitoring members' behavior has been established.*

Elinor Ostrom: Design Principles of Common-pool Resource Institution

- *A graduated system of sanctions is available.*
- *Community members have access to low-cost conflict-resolution mechanisms.*
- *Nested enterprises — that is, appropriation, provision, monitoring and sanctioning, conflict resolution, and other governance activities — are organized in a nested structure with multiple layers of activities.*

Pooling Personal Data

- Where is the boundary?
- What are the rules? Who make them?
- Can the rules be changed? How?
- Is the pool recognized and respected?
- What happens when the rules are breached?
- How about free riders? What are the incentives to pool together? How to monitor and sanction?
- How to resolve conflicts?
- Small pools, large pools, many pools!

Scheduling Group Meetings – An Example

- “Let's decide on a time to eat at this new pasta place!”

- How to pool preferences and make decisions
  - without revealing unnecessary personal information
  - while participants can validate the process and the result
- A community adhering to good practices of data sharing shall re-enforce a sense of being in a good community.
  - An expression of preference can be viewed as a commitment (e.g. people shall show up at the place if they pick the time)
  - Norms and governance issues

Data Pooling: More Scenarios

- Aggregation and sharing of health and medical history from and for a group of people for mutual and public benefits
  - Travel history e.g. in the time of a disease outbreak
  - Where did you go to? Whom did you meet, and when?
- Communal sharing of personal transportation routes
- Group buying decisions, etc.

Methods for Sharing Sensitive Information

- Secure multi-party computation
  - methods for multiple parties to jointly compute a function over their private values without revealing them
- Open-audit e-voting
  - protocols and systems for online voting in which each voter gains assurance that his or her vote was correctly cast, and any observer can verify that all cast votes were properly counted
- User-centric online services
  - personal data is stored on servers that act as intermediaries to other online services; personal data is only sent on a need-to-know basis

Mastodon – a case study

- Many people are not happy with Twitter
- Mastodon: open source software for microblogging
  - Self-hosted or community-run social media platforms
  - Federated: cross-platform “follow”, “reply” & “like”
  - No advertisement, nor biased curation of interactions
  - Platforms can craft their own Terms of Service
  - Ideal as coop platforms with good data governance
- “Between 800,000 and 1,5000,5000 users on between 1,200 and 2,400 instances.” (2017-08-17)

social.coop – a case study

- https://social.coop/about
- “What makes social.coop different from other Mastodon instances?
  - Your data in a place you control and trust
  - Cooperatively co-own the instance
  - Co-create policies, code of conduct, etc (see our bylaws)
  - Democratically run our operations (see our Loomio group)
  - Co-finance expenses transparently (see our OpenCollective page)
  - Participate in a #platformcoop case-study
  - Join a community of like-minded people”

Toward A Participant-Centric Governance Framework

- A participant-centric framework where members of the community can choose how and whether to share their data.
- Relying not only on an effective information system for individual decisions, but also on the process of commoning through which a collective identity is formed.
- Making sure that the entire community will be protected and benefited.