This document: https://tinyurl.com/hackcovid-group1

hackCOVID Group 1 (Data Protection)

Aims of this group:

- Contracting between different entities → Data Commons as an intermediary
- Understand the privacy impact → Risk mitigation measures

Data Commons Assumptions

- A construct whereby the data itself, or connections to the data, is controlled by the commons--people who have data in the commons
- In our case, it would be COVID-19 related information about individuals
- The data is provided by individuals or their devices or their healthcare providers
    - Geo-location data provided by an individual from their mobile devices
    - Blood tests provided by healthcare providers
- Pointers to the data reside in the commons
- Access to my data in the commons
    - I always have access to my data
    - someone else may access my data if allowed by the commons (rule-based, for example)

Concerns

- Government involvement
    - Uptake by government
    - Can we trust the government? No ;-)
- Data commons needs to be (requirements):
    - Trust-creating
    - Easy to use for people willing to upload data
    - Useful enough to the government so that forceful intervention is unneeded
    - Discouraging for the emergence of a dominant app
        - Need standards that will distribute the data
- Data Commons usefulness aspects (design considerations):
    - Aspect 1: Handle data and do everything with it
    - Aspect 2: Showing an alternative viable path
        - If the urgency was lower, could we have created a better model
    - Aspect 3: Make the case for a sufficient level of government access
        - What data can help us assess how much state surveillance is necessary?
        - Proportionality of the scope of access given to the state
    - Aspect 4: Super-national level perspective (UN)
        - Need to make more clear to the global organization the importance of their involvement in how governments handle citizen data
    - Aspect 5: Protect our privacy from other non-government companies
        - Telcos

        - Mobile apps collecting geolocation data
        - Web trackers
- Data Commons short-comings (sufficiency):
    - Is our collective data enough?
    - If not, how do we involve parties that we need data from?

Challenges

- Review from privacy/ethics standpoint
    - our own brainstormed tech development idea solution
    - Data flow/process model from other groups
    - Literature/diagrams from other groups
- Risk Mitigation using legal/technical strategies
    - Troubleshoot in advance foreseeable potential pitfalls
    - Build a prototype of a part of this and show how it would work
    - Clarify the full cycle while taking into account all parties
- Document supporting evidence
    - Find an actual case where we can reduce the need for government to forcefully access data

Discussion Points

- Which circumstances necessitate consent/when can other legal tools be used instead
    - technical/policies for being transparent in cases where government practices power to access personal data without consent
    - National security is about having target groups of people
    - COVID-19 → Threat Model is a natural disaster - a non-targeted threat to the entire population
- Identify parties that can handle the data
    - Need to deliver accurate data to the parties that are fighting the virus on the front line
    - Need to limit the consequences afterward
        - Need rules about what happens afterwards
    - Secure multi-party platform can facilitate this
        - Data commons can be a temporary platform that is deleted afterwards
- Data Commons as a solution
    - A calculation can be brought into the platform (only results go out)
    - Feasibility may be questionable
        - Updates from telcos possible? → Data Commons would actually pull data from individuals' phones rather than telcos
        - May be difficult to pull together in time for COVID-19, but it will be useful for the future of humankind
        - The government may prefer to use other intermediaries that are not designed with privacy in mind
    - How to propose a way that can be used for COVID-19?
        - We can become the proof of concept
        - JLINC interface allows selective disclosure, might be useful now

            - B-service (government, requestor) side asks for certain kinds of data
            - A-service (individual) decides to share
            - An audit trail is recorded (notification to the subject of contact-tracing)
            - Example: Speed to access to data Korea case
    - Considerations for Intermediary acting as a fiduciary
        - responds appropriately when the state approaches with a public concern
        - Collective
        - Recognizing the role of the state, at time overriding privacy concerns
            - This should be clear for the individual to understand
        - Outbound side:
            - An intermediary can provide the “aggregated data” the government wants while eliminating the need for the government to look at individual-level personal data
            - Ex) Telcos, credit card companies, supermarkets may have provided my data to the government, but if so, how can I know?
        - Inbound side:
            - Level 1: Self-reporting actors only (for MVP)
                - Allow for people to ask telco to disclose their data
            - Level 2: IoT devices (thermometer)
            - Level 3: Lab result with reference to the lab
            - Level 4: Health authority reporting
    -

    - Scenarios of abuse are of concern and should be addressed
        - What are the conditions that allow for the government to invoke GDPR Article 6.1(e)? https://gdpr-info.eu/art-6-gdpr/
            -
- Question: Is the data commons for COVID a temporary construction for the duration of the crisis, or an enduring construct?
    -

- JW: The amount of trust that the individual has in the ability of the data commons (the intermediary) to more likely they are to participate and to accurately self-report. If individuals don’t trust, they will lie or obfuscate, which will skew the data.
    -
- GDPR case:
    - Article 6 (b) contract as the basis for participating
    - Article 6 (e) public interest in releasing data

JW: Possible Framing of the Response (Data Commons)
Business: What is the form of the Data Commons Entity? NGO, Benefit Corporation, For-Profit entity, etc.

This document: https://tinyurl.com/hackcovid-group1

Legal: What are the terms of the ‘trust”? (fiduciary, controller, intermediary)
Technical: Group 2
Social: What are the commitments of the Data Commons Entity?

JW: Use Cases for Data Protection

- Orthogonal is Jurisdiction (is this legal?)
- Scope of the collection (what is collected?)
- What do we want to do with this data?
- Can we make effective use of the data?
- Who has access to static data?
- How is computation structured?

Who has access to static data?

Hypothesis: if we can preserve the functionality, we need to lower the access-level needed as much as technically feasible

UC1: Local Storage and Control (App)

- API access to data for reporting
    - Aggregate (anonymous)
    - Pseudonyms (mapping)
    - Individual (with authority or permission)

UC2: Controlled Storage & Access (MyData Commons)

    - Aggregate (anonymous)
    - Pseudonyms (mapping)
    - Individual (with authority or permission)
    - Need a balance in pseudonymity to defer government from wanting more access

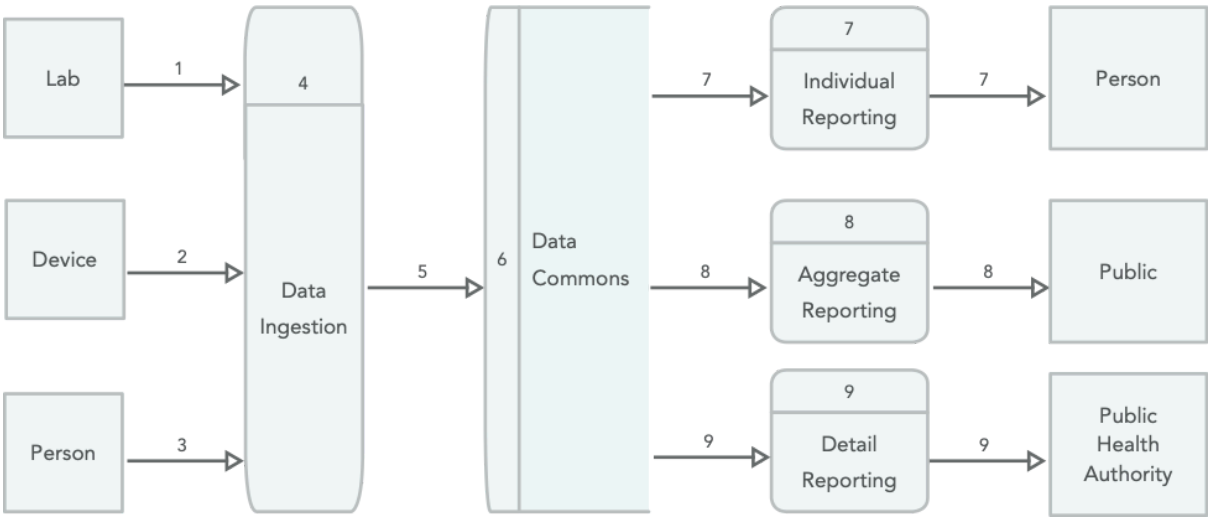
UC3: Consented Database (traditional)

    - Aggregate (anonymous)
    - Pseudonyms (mapping)
    - Individual (with authority or permission)

UC4: Mandatory Pull by Authorities

    - Aggregate (anonymous)
    - Pseudonyms (mapping)
    - Individual (with authority or permission)

This document: https://tinyurl.com/hackcovid-group1



Who can compute on data?

Data Commons Policies/Dataset/Parameters?

Relative advantages

Considerations

- Thinking about social dimension (data about multiple people)
-

References

Contact tracing to control the infectious disease: when enough is enough https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3428220/

JLINC Protocol https://protocol.jlinc.org

Bottom-Up Data Trusts https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3265315

This document: https://tinyurl.com/hackcovid-group1

-