Key Points from Day 3 (Thursday, January 19) [DRAFT]

Understanding the mechanisms driving variable, non-exponential patterns in epidemics is necessary to accurately forecast future outbreaks.

1. Real epidemics exhibit variable epidemic growth scaling due to mode(s) of transmission, reactive behavior changes, spatial effects, and individual-level heterogeneity in susceptibility and infectiousness.

2. Ensemble sub-epidemic models can capture complex transmission dynamics, including fluctuations in epidemic waves over time.

3. Sub-epidemic modelling frameworks have been shown to outperform similar infectious disease models (e.g., ARIMA models of COVID-19 in the USA), and hold potential for forecasting other biological and social growth processes.

Nascent cryptographic tools can enable secure computation on joint datasets in a privacy-preserving way.

1. Secure multi-party computation (MPC) can enable multiple parties (e.g., via secret sharing, two-server secure aggregation) to perform a computation for output generation without disclosing any individual's inputs.

2. Zero-knowledge proofs (ZKP) are a special case of MPC. ZKPs allow one party to convince another party that a given computation or output is true without revealing any identifiable information.

3. In extreme cases, an individual's identity could be inferred from MPC outputs. There is potential to pair MPC with differential privacy techniques to further reduce privacy threats.

Key Points Re: MAPPING@Brown

1. Epidemic simulation scenarios based on MAPPING@Brown data could choose to rely on graphical networks, locational data, or contact matrix data. Graphical network data have the potential answer questions related to space/location that contact matrices cannot.

2. Analytical methods for network analysis could include simulating the MAPPS network data using semi-mechanistic models, Exponential Random Graph Models, classic ensemble models, or an ensemble of ERGMs. Any simulation(s) should be guided by policy-relevant hypotheses.

3. MPC protocols that utilize two servers for secret sharing and computation of MAPPS data have the potential to increase data sharing efficiency and will be favorable from an IRB perspective.

4. MAPPS data can be used to improve our understanding and measurement of networks in multiple ways, such as measuring how long individuals have been in contact with specific fomites or whether there are associations between proximity to specific locations (e.g., bathrooms) and pathogen spread.