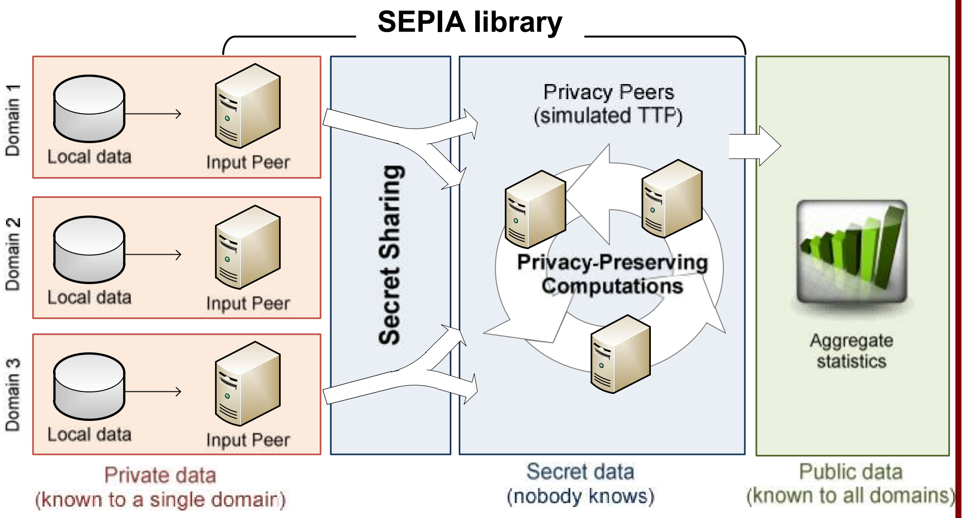
Topic 3-4: Integration of Technologies and Legal, regulatory, privacy aspects.

Approach: Multi-Party Computation



Characterize the type of data it can aggregator or correlate.

- SEPIA's MPC protocols: Event Correlation, Distinct Count, Top-k Reports, Entropy, Vector Addition.
- The protocols:
  - are inspired from network security/monitoring applications
  - are general-purpose operating on input vectors of scalars
- SEPIA's crypto foundation is efficient MPC comparison operations

State the benefits

- MPC provides a good solution to the privacy – utility tradeoff
- MPC is a better alternative than anonymization for collaborative data sharing
- MPC can be used when Trusted Third Parties are not a option.

Timeline / roadmapping

- SEPIA library is presently publically available:

sepia

http://www.sepia.ee.ethz.ch

- Various extensions under development, e.g., set intersection protocol

Xenofontas Dimitropoulos/Martin Burkhart @ ETH Zurich