Cryptographically Protected Computing

Mayank Varia

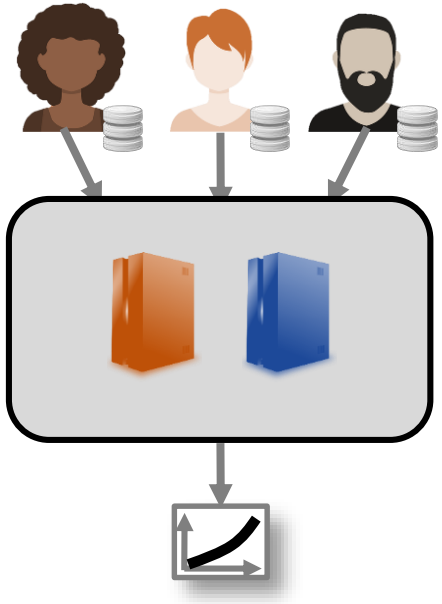
Boston University Computer Science

BOSTON UNIVERSITY

Protecting computation

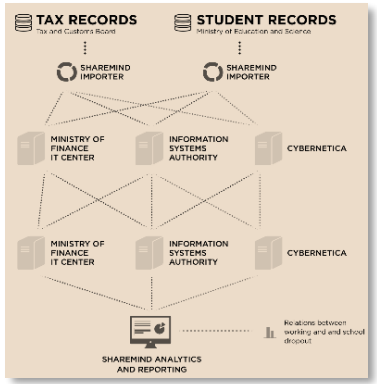
"Secure multi-party computation… enables different participating entities in possession of private sets of data to link and aggregate their data sets… without transferring or otherwise revealing any private data to each other or anyone else."

– 2019 U.S. Senate bill S.681

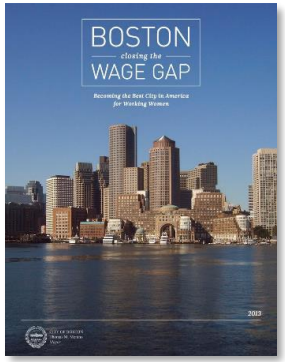


Selected deployments of SMC (bit.ly/33p7Rgy)

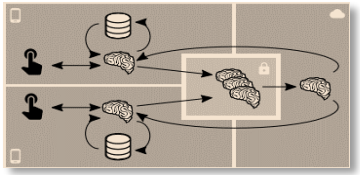
Cybernetica: Education outcomes



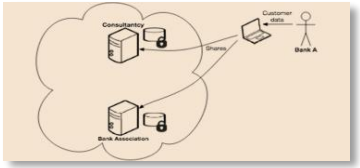
BU: Pay equity in Boston



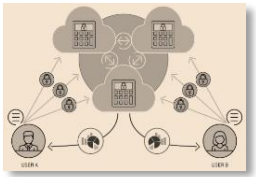
Google: Federated learning



Partisia: Rate credit of farmers

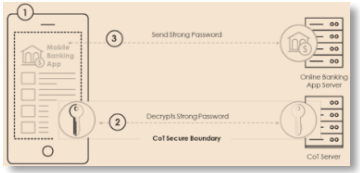


Statistics Denmark: Energy efficiency



Callisto: MeToo harrassment

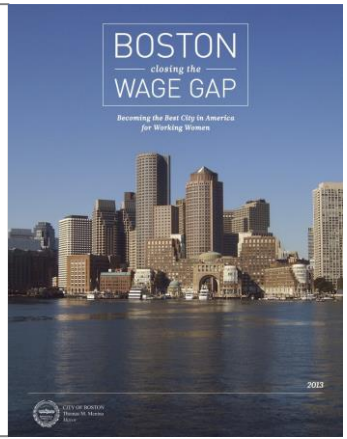
Unbound + Sepior: Protect crypto keys



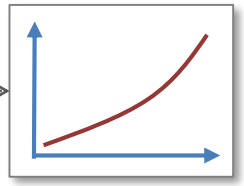
BOSTON UNIVERSITY

Boston Women's Workforce Council wage gap study

Goal 3: **Employers agree to contribute data** to a report compiled by a third party on the Compact's success to date. **Employer-level data would not be identified** in the report.



Logical workflow



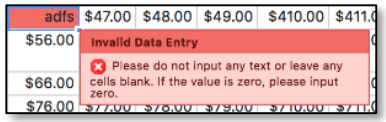
	Hispanic or Latinx		White		Black/African American	
	Female	Male	Female	Male	Female	Male
Executive/Senior Level Officials and Managers						
First/Mid-Level Officials and Managers						
Professionals						
Technicians						
Sales Workers						

BOSTON UNIVERSITY

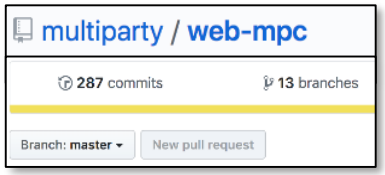
Providing value to all stakeholders

HR Personnel
Accessibility

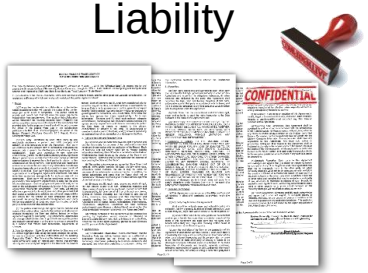
BWWC
Accuracy



IT Personnel
Auditability



Lawyers
Liability



BOSTON UNIVERSITY

Law and policy question

Is protected computing permissible when data is encumbered by privacy laws? Let's stipulate that the output (on its own) would be legal to disclose

- *Definitional question*: do encoded pieces count as personal data?
- *Process question*: does computing over encodings constitute disclosures?
- *Liability question*: who should be blamed if there is an error?