Brandeis Program

Dr Josh Baron
Program Manager

ACSAC big data privacy panel

12/06/2017
Develop tools and techniques to enable the building of information systems where private data can be used for the intended purpose – and no other.
Brandeis System Concept

Data Owner

Human Data Interaction (TA2)

Privacy Policy User Interface
(Users define and understand policy)

Experimental Integration Platforms (TA3)

Privacy Preserving Techniques
(Encryption, MPC, Differential Privacy)

Privacy Measurement (TA4)
(Metrics for measuring privacy protection)

Data Requester / User/ Analyst

Data requesters use, analyze privacy protected data
Privacy-Enhanced (PE) Android

**PE Android with RapidGather App**

**Prototype simple interface for privacy decisions**

Infer user privacy prefs

Crowdsources privacy reasoning

Source: Raytheon BBN

Source: CMU
Coalition Information Sharing

Policy-differentiated Information Access:
- Different content and resolution based on privacy policies for different community, national, and international roles

International Response Coordinator: nation-level view, but no community level details

Cebu City Coordinator: community-level view only

Bohol Coordinator: community-level view for Bohol, nation-level view for others
Building testbed for researching and experimenting with privacy technologies:

- Physical and virtual sensor feeds
- API for rapid creation of privacy preserving apps that integrate with building sensor data
- Integration of diverse privacy-preserving compute & storage technologies