

Welcome

Actionable Intelligence for Social Policy (AISP)

School of Social Policy & Practice

University of Pennsylvania



Plenary 4

Key Topics in privacy-preserving technologies: What is PPT and how can it support integrated data sharing efforts?

Amy O'Hara

Research Professor, Massive Data Institute



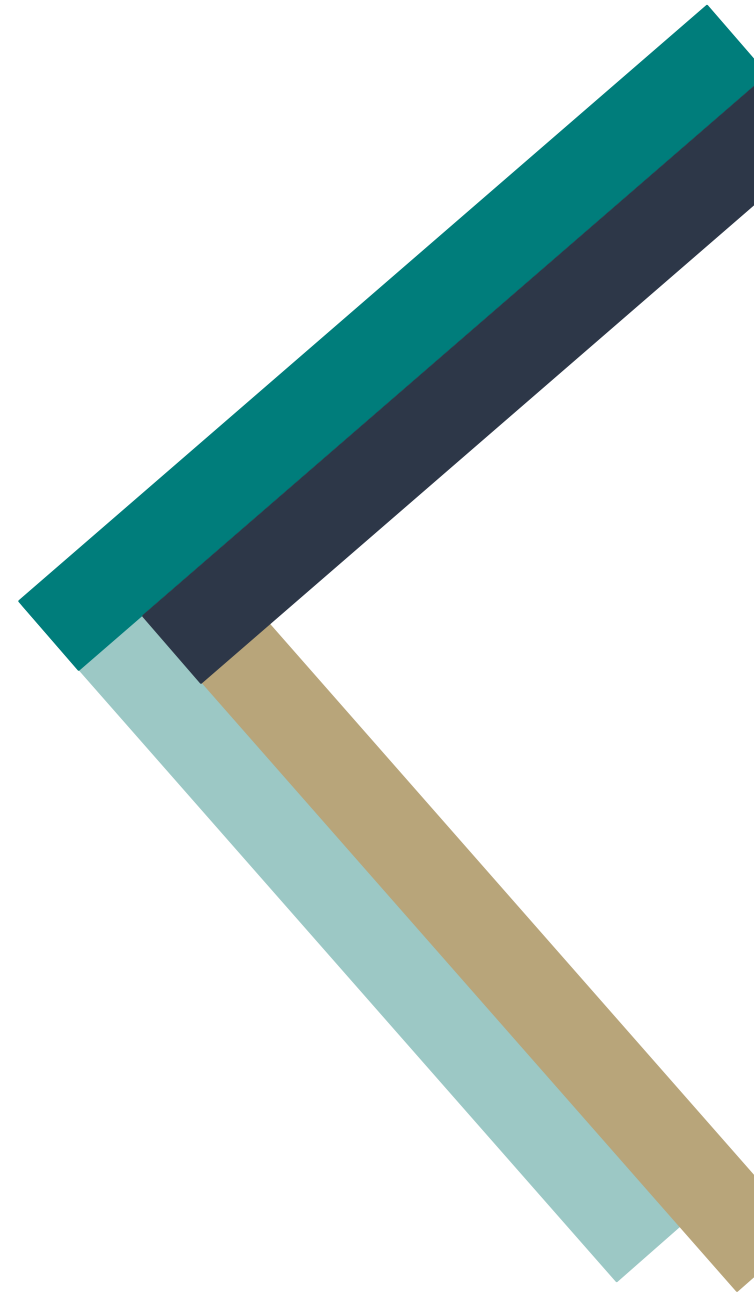
Aaron Bean
Managing Partner, Asemio

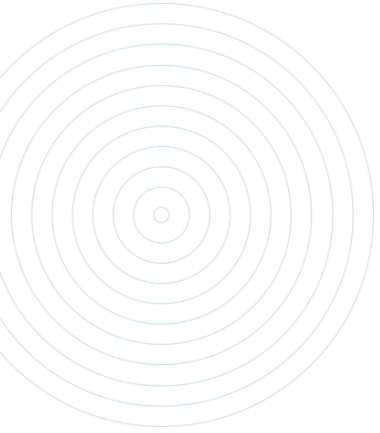


Key Topics in Privacy Preserving Technology

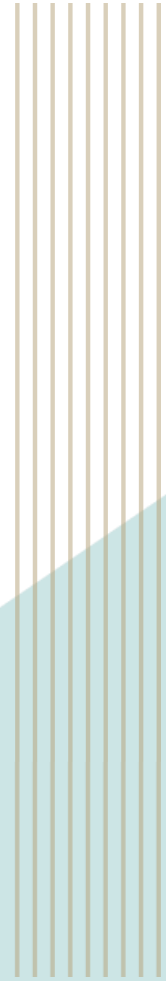
What is PPT and how can it support
integrated data sharing efforts?

Dr. Amy O'Hara, *Georgetown University*
Aaron Bean, *Asemio*





What are PPTs and where do they fit into the privacy landscape?



DEFINITION

What are
**privacy preserving
technologies?**

PRIVACY PRESERVING TECHNOLOGIES (PPTs)

Also referred to as privacy-enhancing technologies (PETs), PPTs are technical approaches that **minimize use of and need for personal data**, including identifiers, **while supporting record linkage through privacy techniques.**

VALUE PROPOSITION

Where do PPTs
fit into the privacy
landscape?

By more *quickly* meeting compliance, legal, and security concerns for extremely sensitive data:

REGULATORY SENSITIVITY

Examples: 42 CFR Part 2 entities, HIPAA/FERPA
crossovers

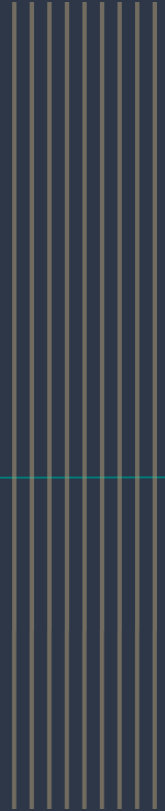
SOCIAL SENSITIVITY

Examples: Domestic violence and legal service
organizations

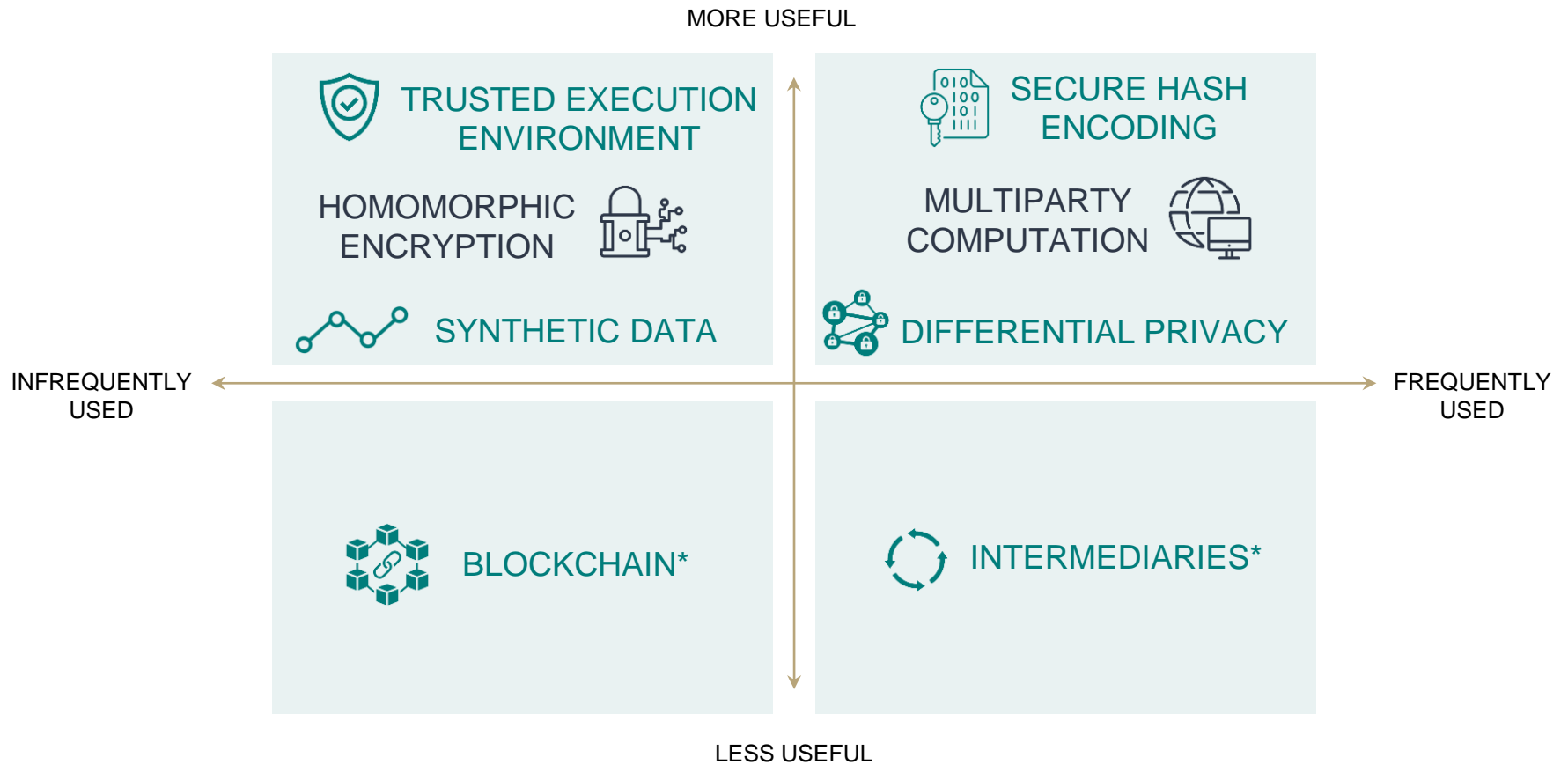
POLITICAL SENSITIVITY

Examples: Tribal, State, and Federal crossovers

Different Methods



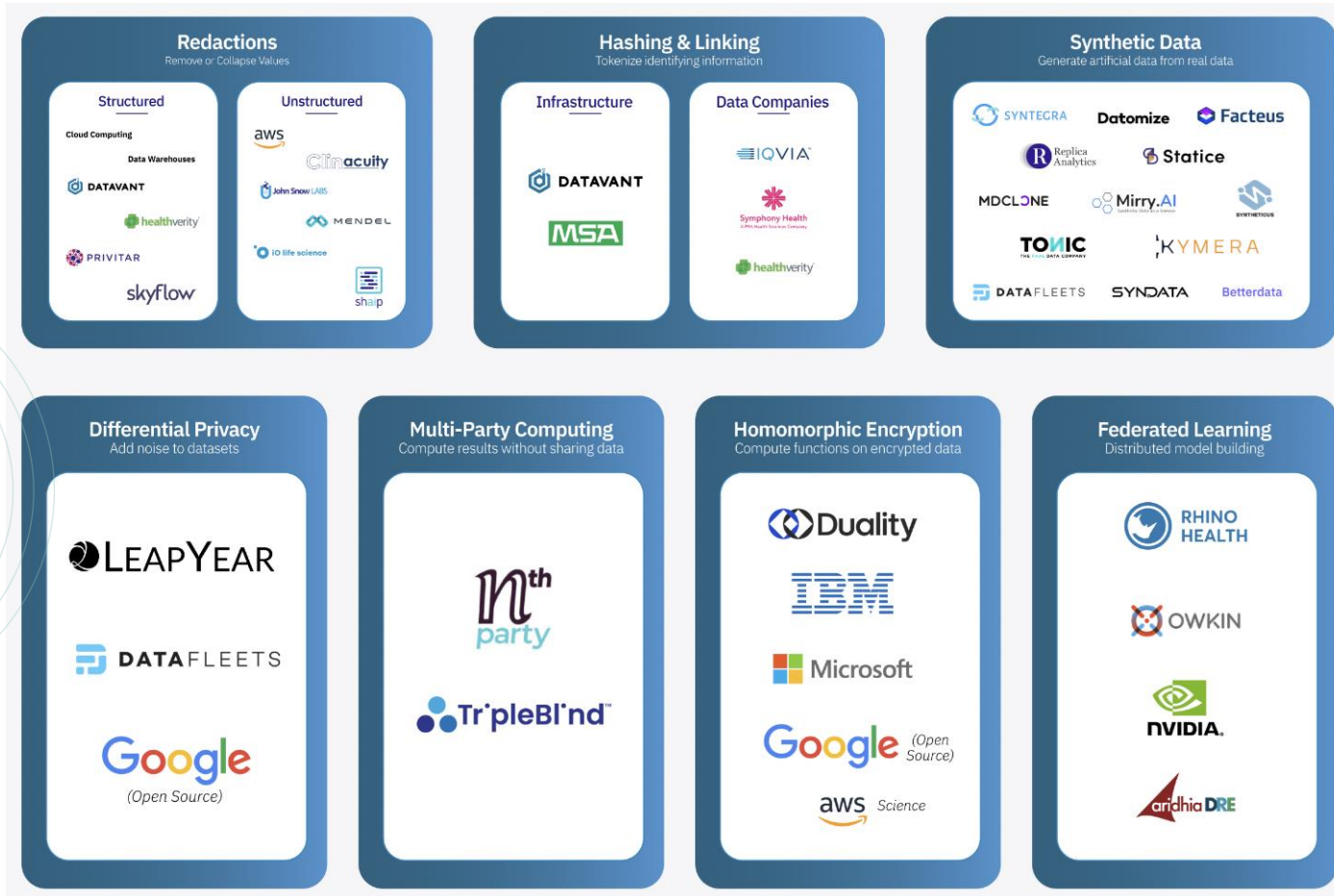
Different PPT Methods



Broader Landscape

A decorative graphic consisting of ten thin, vertical, light-colored lines arranged in a column on the right side of the slide.

Privacy Preserving Technology Landscape



Graphic Credit:
[Datavant](#)

Application to Government

A decorative graphic consisting of ten thin, vertical, light-colored lines arranged in a column on the right side of the slide.



GEORGETOWN
UNIVERSITY

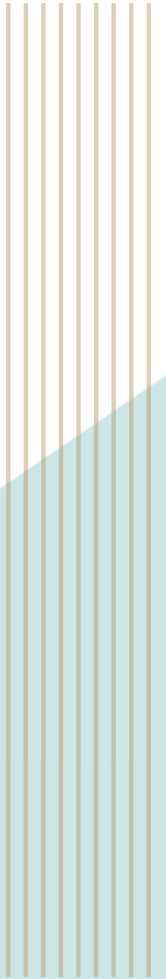
McCourt School of Public Policy



MASSIVE
DATA
INSTITUTE

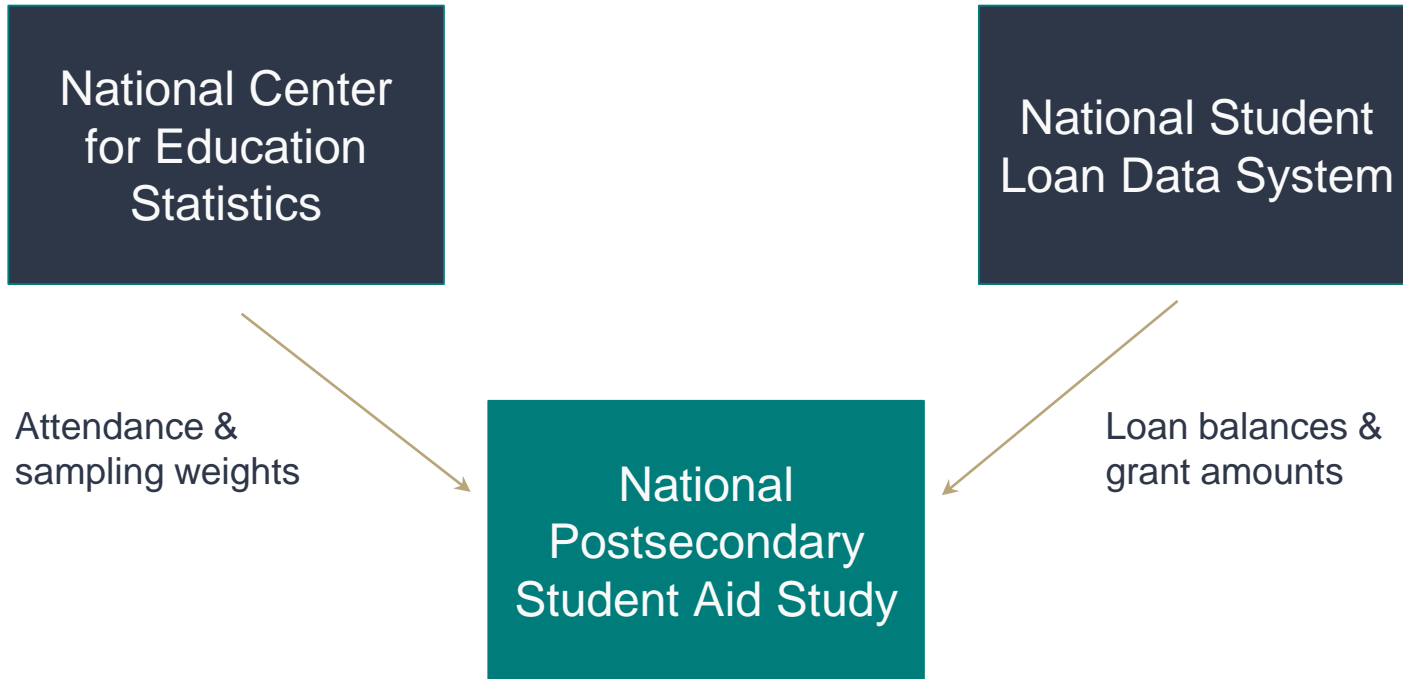
CASE STUDY

WORKING AT THE **FEDERAL LEVEL**



- Push for inter-agency data sharing
 - The Federal Data Strategy (FDS)
 - Foundations for Evidence-Based Policymaking Act of 2018 (H.R.4174)
- Hampered by privacy policy, statute, and practice of agencies
- Current privacy approaches carry risks
- Solution → Privacy Preserving Technologies (PPTs)
 - Secure Multiparty Computation (SMC)
- Supported by the Alfred P. Sloan Foundation

Current NPSAS Structure (SMC)



Potential NPSAS Structure

National Center
for Education
Statistics

→
Encrypted
Attendance &
sampling
weights

SMC

←
Encrypted
Loan balances
& grant
amounts

National Student
Loan Data System

↓
Decrypted
results

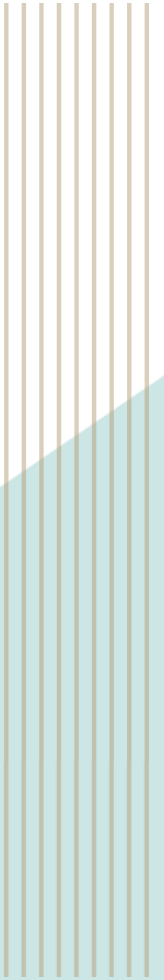
National
Postsecondary
Student Aid Study

- Successful privacy preserving, inter-agency data sharing
 - Privacy preserving
 - Accurate
 - Efficient computation and network costs for real, full-scale data
 - Cost-effective
 - Easy to use
- Some challenges remain
 - Certification of software components
 - Legal & technical concerns
 - Introduction into workflow

asemio

CASE STUDY

WORKING AT THE **COMMUNITY LEVEL**



A crucial element of collaborative action is **using data to continually learn, adapt, and improve**, but this goal can prove difficult to achieve due to:

- complex, drawn out governance cycles,
- disparate technology systems,
- and varying levels of experience and resource availability.

Community stakeholders focused on improving childhood outcomes came together to achieve actionable insights in weeks instead of years.

- Eight organizations representing 32 programs contributed data from a 12-year period **to answer community-level questions regarding race, equity, and service overlap.**

FEATURED PARTNERS

blue meridian

partners

GEORGE KAISER
FAMILY FOUNDATION
A supporting organization of Tulsa Community Foundation

BIRTH THROUGH
EIGHT
STRATEGY FOR
TULSA

Challenge

Early approaches focused on the creation of a centralized data warehouse, believing this would offer a simpler, straightforward path for data sharing.

This one-size-fits-all technical approach required months to navigate the legal landscape and sought to achieve buy-in for a long-term vision that was still in development.

Progress was slow and placed a time and energy burden on data contributors who received little immediate benefit.



APPROACH

Federated
Governance



TECHNOLOGY

Privacy Enhancing
Technologies



TEAM

Cross-sector
Tech + Public Interest

“Something that has been absolutely vital and extremely helpful has been how flexible the Asemio team has been about accommodating the needs of the partners involved.”

– MONICA ROGERS, *Tulsa Health Department*

“By more easily meeting compliance requirements that are necessary for this process, you invite more partners to the table.”

– DAN STERBA, *George Kaiser Family Foundation*

Community Level **Success** with Data Sharing

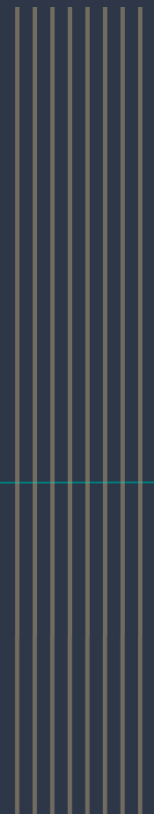
“How do we make data sharing **easier** and **more accessible** in Tulsa?”

THE RESULTS

Data from a **12-year period** accessed from **32** programs
Participation from **8** organizations
Insights to **5** community questions
1/2 the time invested when compared with traditional methods

... all achieved in **2 months' time**

Limitations



PPT Limitations*

- Complexity
- Cost
- Unintended Consequences
- Uncertainty
 - Lack of familiarity
 - Lack of regulation

**Diversity of techniques means limitations are different across the spectrum*

Future Areas of Interest

A decorative graphic consisting of ten thin, vertical, light-colored lines arranged in a column on the right side of the slide.

Future Areas of Interest and Study

- Clarify the value of PPTs
 - Enhanced use cases
 - Improved reference architecture
 - Evolved legal briefs
 - More input on social license from community members
- Demonstrate the value
 - Invest in, and advocate for, demonstration projects
 - Get creative on partnerships
 - Develop additional case studies, and talking points

Q&A

Thank you!

