18734: Foundations of Privacy

Privacy as Restrictions on Personal Information Flow

Anupam Datta

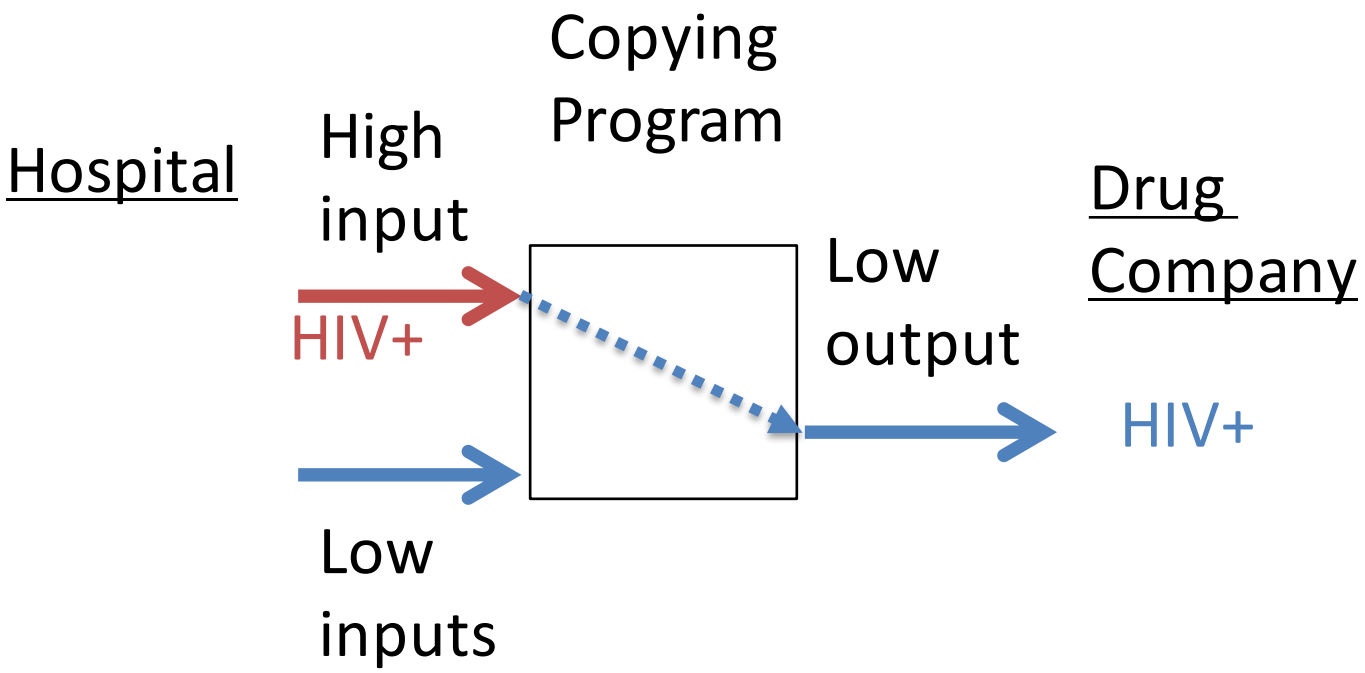
CMU

Fall 2016

Organizing Viewpoint

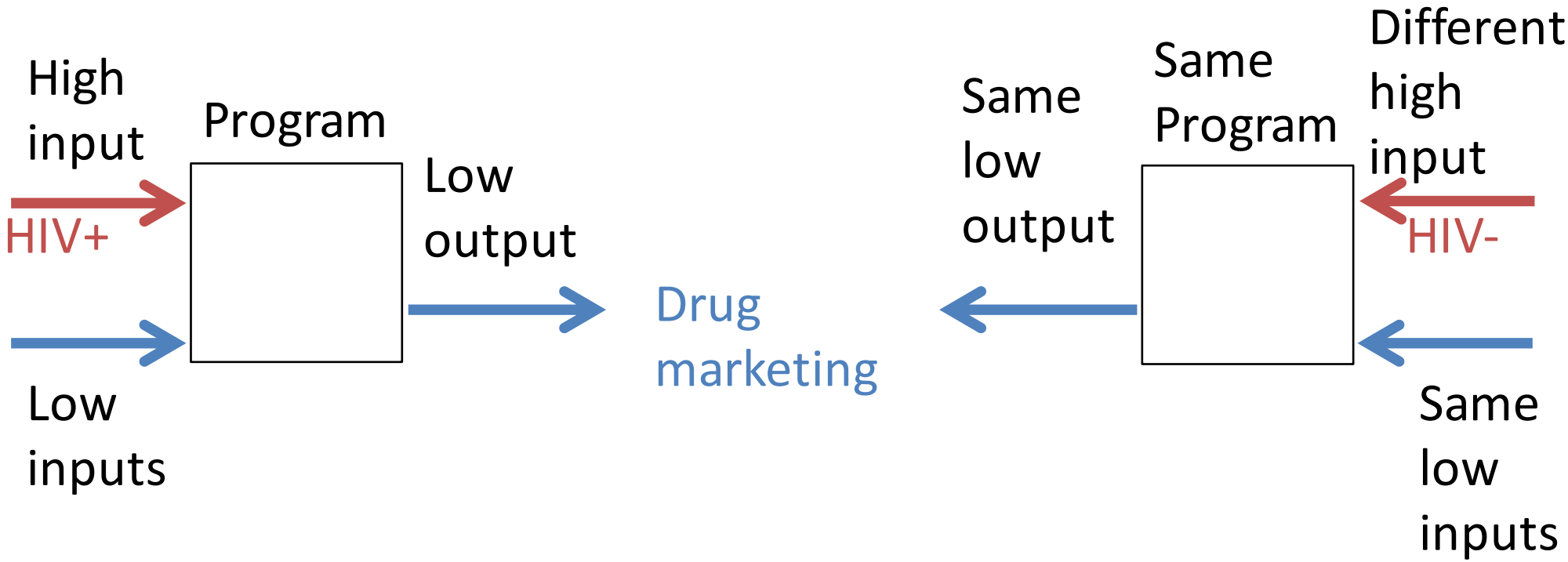
Privacy as a right to restrictions on personal information flow

Direct Flows

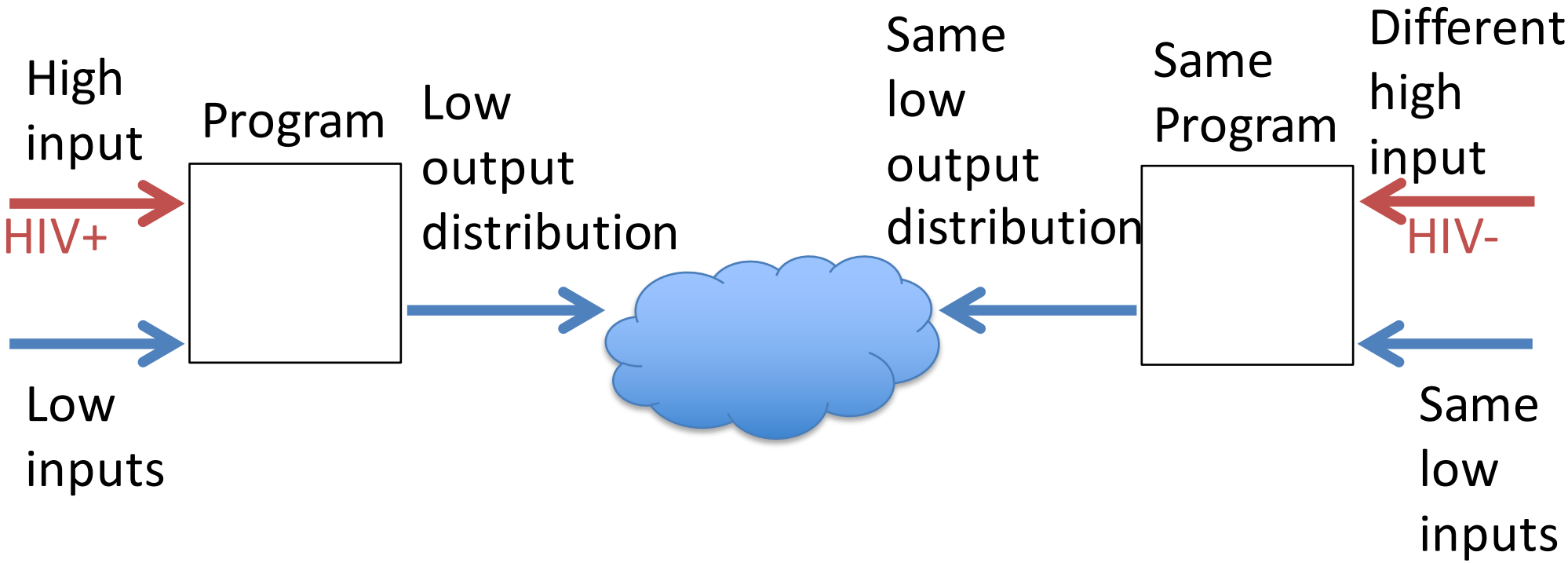


[Goguen and Meseguer, 1982]

Noninterference

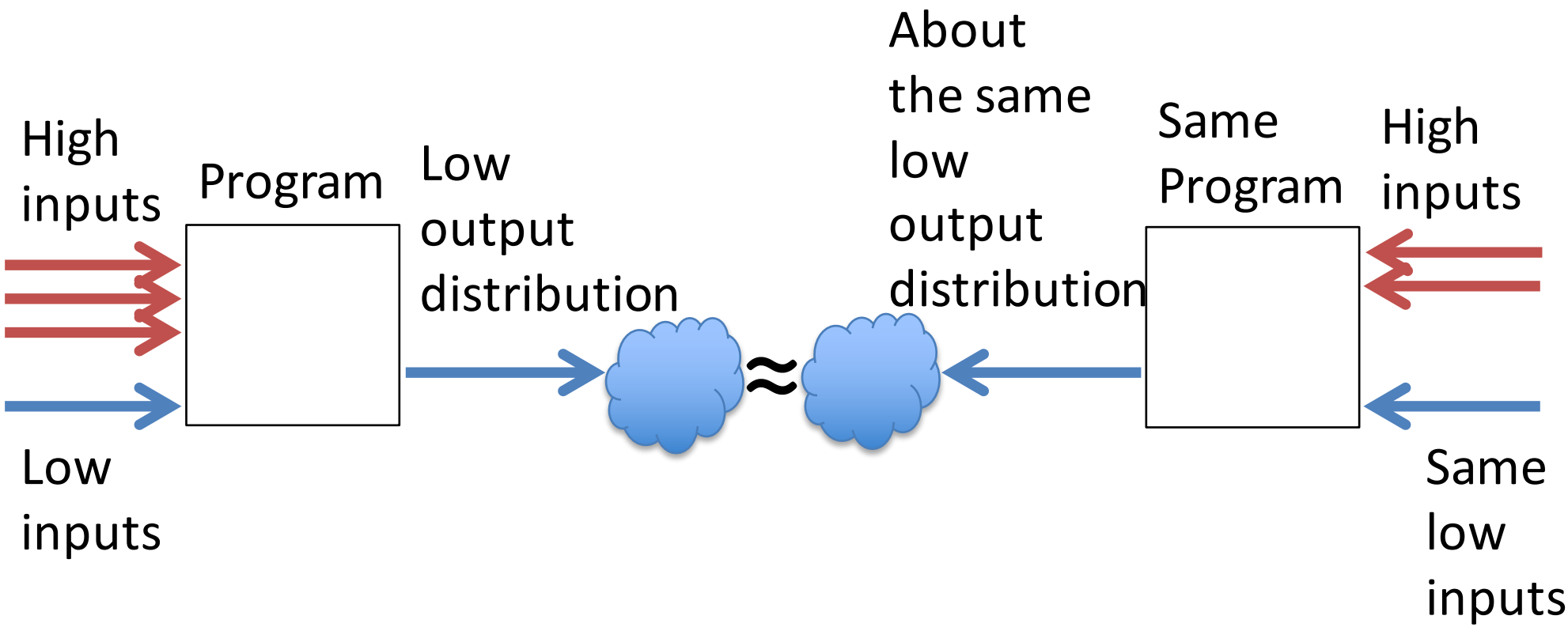


Probabilistic Noninterference



[Dwork, McSherry, Nissim & Smith, 2006]

Differential Privacy



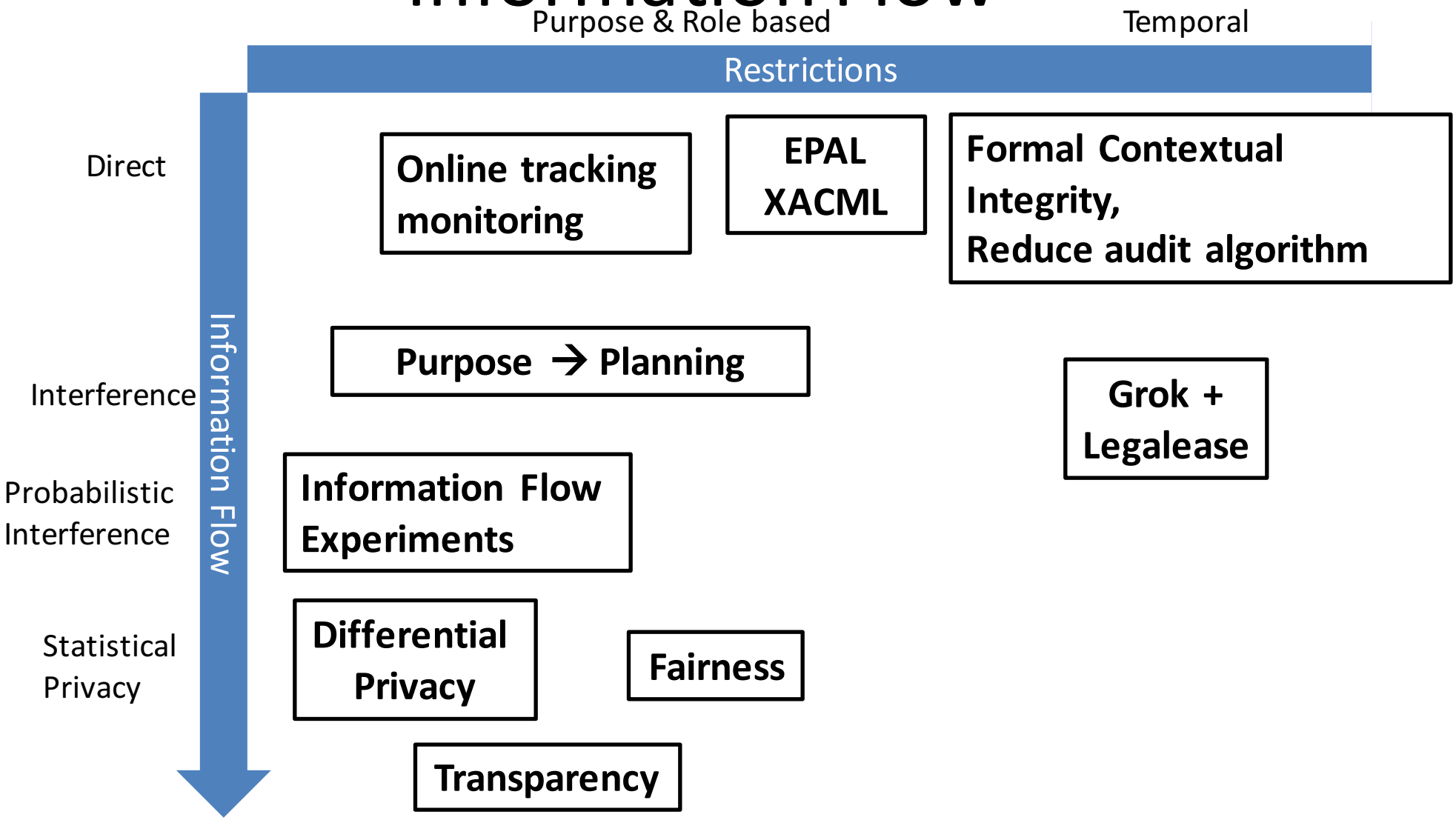
Example from HIPAA Privacy Rule

A covered entity may disclose an individual's protected health information (phi) to law-enforcement officials for the purpose of identifying an individual if the individual made a statement admitting participating in a violent crime that the covered entity believes may have caused serious physical harm to the victim

- Concepts in privacy policies
  - **Actions:** send(p1, p2, m)
  - **Roles:** inrole(p2, law-enforcement)
  - **Data attributes:** attr_in(prescription, phi)
  - **Temporal constraints:** in-the-past(state(q, m))

  - **Purposes:** purp_in(u, id-criminal))
  - **Beliefs:** believes-crime-caused-serious-harm(p, q, m)

Privacy as Restrictions on Personal Information Flow



Big Data: Seizing Opportunities, Preserving Values

Big Data Anaytics Threats to Values

- Privacy
- Fairness
- Transparency

Application Domains

- Public sector
  - Healthcare delivery
  - Education: Learning about learning
  - Homeland security and law enforcement
- Private sector
  - Advertising-supported ecosystem
  - Data brokers

Recommendations (1)

- Preserving Privacy Values: Maintaining our privacy values by protecting personal information in the marketplace, both in the United States and through interoperable global privacy frameworks;

- Educating Robustly and Responsibly: Recognizing schools—particularly K-12—as an important sphere for using big data to enhance learning opportunities, while protecting personal data usage and building digital literacy and skills;

- Big Data and Discrimination: Preventing new modes of discrimination that some uses of big data may enable;

Recommendations (2)

- Law Enforcement and Security: Ensuring big data's responsible use in law enforcement, public safety, and national security; and

- Data as a Public Resource: Harnessing data as a public resource, using it to improve the delivery of public services, and investing in research and technology that will further power the big data revolution.