SAFE-PASS: Stewardship, Advocacy, Fairness and Empowerment in Privacy, Accountability, Security, and Safety for Vulnerable Groups

Indrajit Ray
Sharad Mehrotra
Murat Kantarcioglu
Steve Simske
Bhavani Thuraisingham
Vijayalakshmi Atluri
Ramesh Raskar
Nalini Venkatasubramanian
Jaideep Vaidya
Indrakshi Ray
Babak Salimi
Vivek Singh

SAFE-PASS: Motivation and Goal

We believe

Vulnerable populations are not fully getting the benefit of tech advances because they do not trust tech

We aim to

Achieve societally responsible secure and trustworthy cyberspace that puts algorithmic and technological checks and balances on the indiscriminate sharing and analysis of data

Who Are the Vulnerable Groups

Secure
media
league
Sandbox
Case
Hacking
Cultural
machines
analysis
undergraduate
Program
Liberal
Privacy
Careers
Gencyber
Disorders
Outreach
Small
Increasing
Summit
Inquiry-Based
gencyber
virtual
Curriculum
forensic
High
National
K-12
psychology
interventions
Learning
Engaging
Course
Evaluation
based
Flag
Active
inquiry
Profiles
multi-institutional
Preparing
Protection
Women
general
risk
course
Cybersecurity
competition
Pathway
introductory
increase
Unplugged
Research
Vulnerabilities
Science
training
Early
Game
Integrating
Tactics
built-in
Engineering
Computational
engagement
Design
science
national
Re-engineering
Undergraduate
longitudinal
Universities
perceptions
Based
Teach
learning
Responsive
role
REU
Concepts
CS
Capture
secure
Enhancing
active
Alternatives
programming
school
Spears
iOS
Interest
Like
Study
Folk
gaps
Scenario-based
European
Cohort
Facilitate
Maryland
peer
Peer
Enabling
Engage
Limited
game-based
Technology
Pedagogy
University
Diversity
Experience
Towards
social
instruction
Mississippi
Competition
Center
personal
Non-technical
high
Mentoring
cyber-security
liberal
study
Across
Flaws
Social
Hacker's
Planning
Phishing
School
Principles
Building
Inter-Disciplinary
interdisciplinary
interest
Participation
Perspective
curriculum
Shields
Authentic
Nobody
program
Handbook
Practice
General
Gender
SandScout
fields
Autism
Novel

Vulnerable Groups – Defining Characteristics

- Susceptible to being unduly influenced by others to a degree that might be detrimental to their well-being
- Inability to make informed decisions and hence requiring proxy/surrogate
- Cannot be independent physically or mentally and hence have limited capability of taking self-protective actions
- Limited in freedom to act, speak or think without hindrances or restraints
- May experience intense fear about safety because of earlier life experiences

Vulnerable Group Categorization

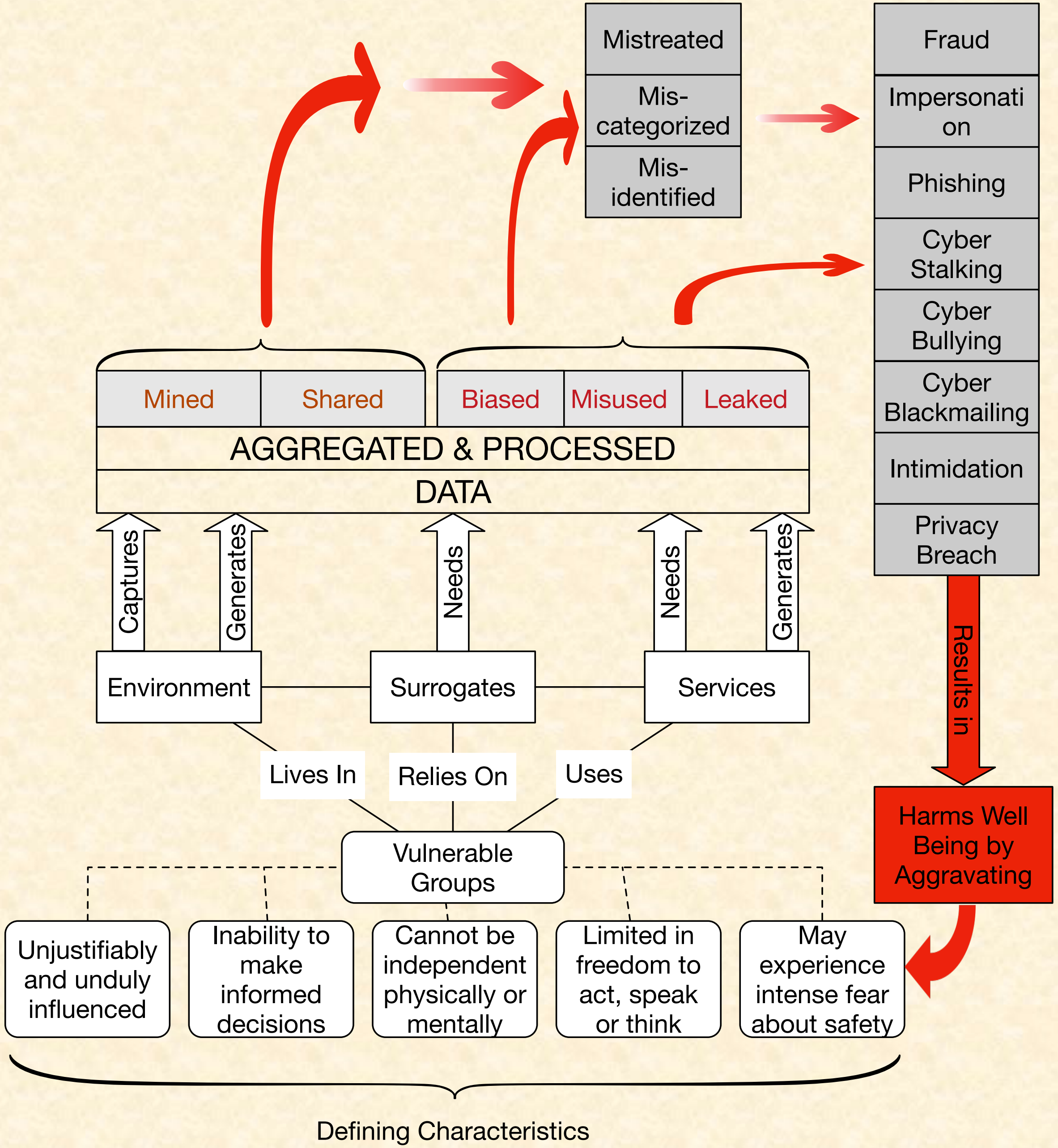
Status as being part of a vulnerable group is not sensitive

- E.g., elderly person living in an assisted living facility

Vulnerable status is itself sensitive and must be hidden to appropriately protect them

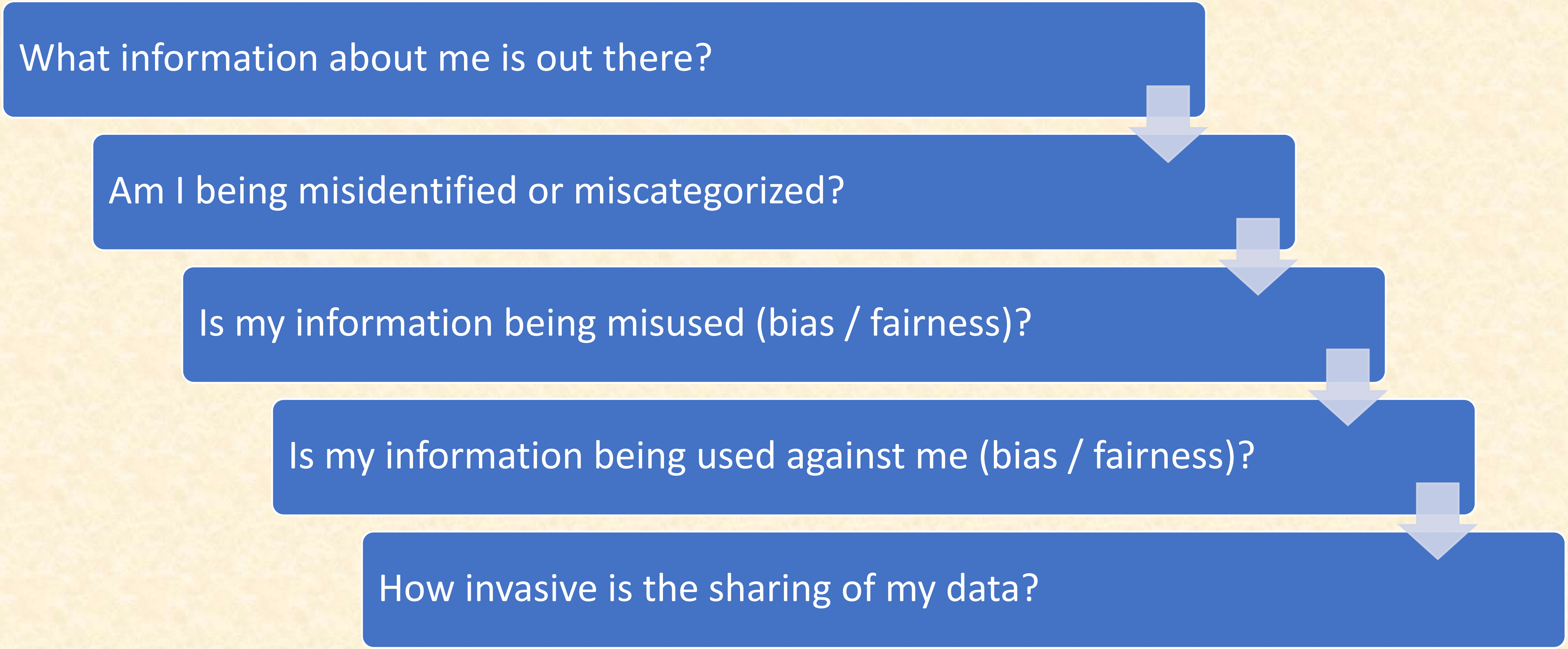
- E.g., victim of human trafficking

The Vicious Life-Cycle of Data Exfiltration, Aggregation and Misuse for Vulnerable Groups



Why Vulnerable Groups Are Most Impacted?

Limited Awareness or Knowledge About Data Sharing and Data Usage



What information about me is out there?

Am I being misidentified or miscategorized?

Is my information being misused (bias / fairness)?

Is my information being used against me (bias / fairness)?

How invasive is the sharing of my data?

Technology Not Specifically Designed for Vulnerable Groups

- No access or limited access to technology
- Left out or victimized by technology
- Inadequate engagement with technology
- Translation or interpretation gap of security and privacy requirement specification when conveyed through surrogates

Less opportunities of inculcating trust in technology

Data Imbalance and Missing Data in AI/ML Techniques

Measurement errors in data

- Vulnerable groups inadequately represented in control groups
- Study questionnaires are often based on societal norms

Results in

- Selection bias
- Misclassification
- Miscategorization
- Misidentification

Vision – New Societally Responsible Data Integration, Analysis & Sharing Paradigm

🔒 Selective Secrecy	Judiciously providing strong levels of security and privacy to shared data by default Updating security and privacy levels based on situational awareness and utility of data sharing
? Structural Transparency	Answering questions about how data is collected, stored and used, if data is biased, is it being misused, etc.

Stewardship, Advocacy, Fairness and Empowerment

Stewardship: Develop technology for selective secrecy and structural transparency for vulnerable groups and guiding them to make informed decisions

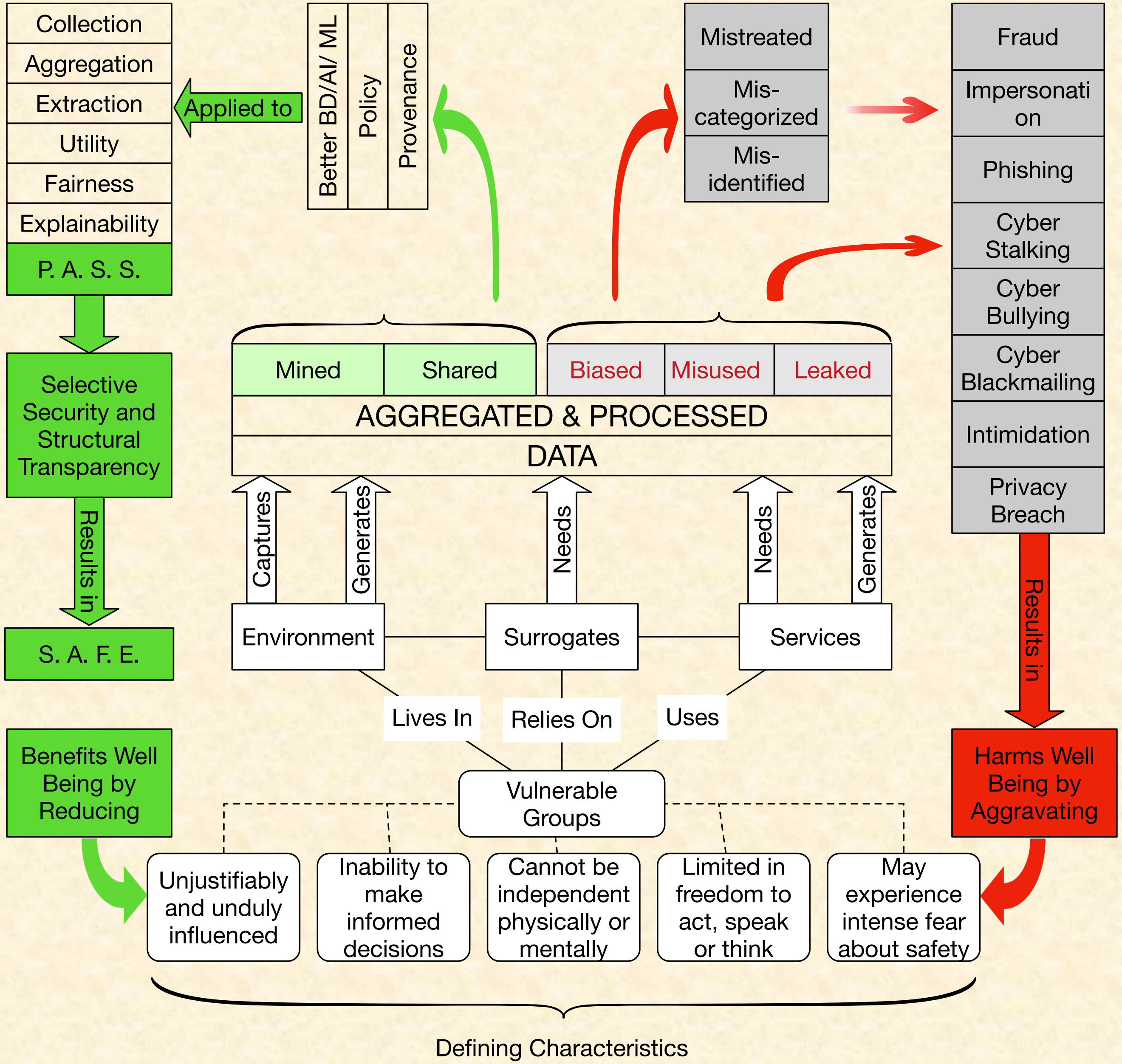
Advocacy: Proactively evaluate technology to raise awareness, identify, develop and adopt best practices, policies and technologies

Fairness: Develop tools and techniques that mitigate biases and augment data to emphasize vulnerable groups

Empowerment: Educate vulnerable groups and enable safe access to information

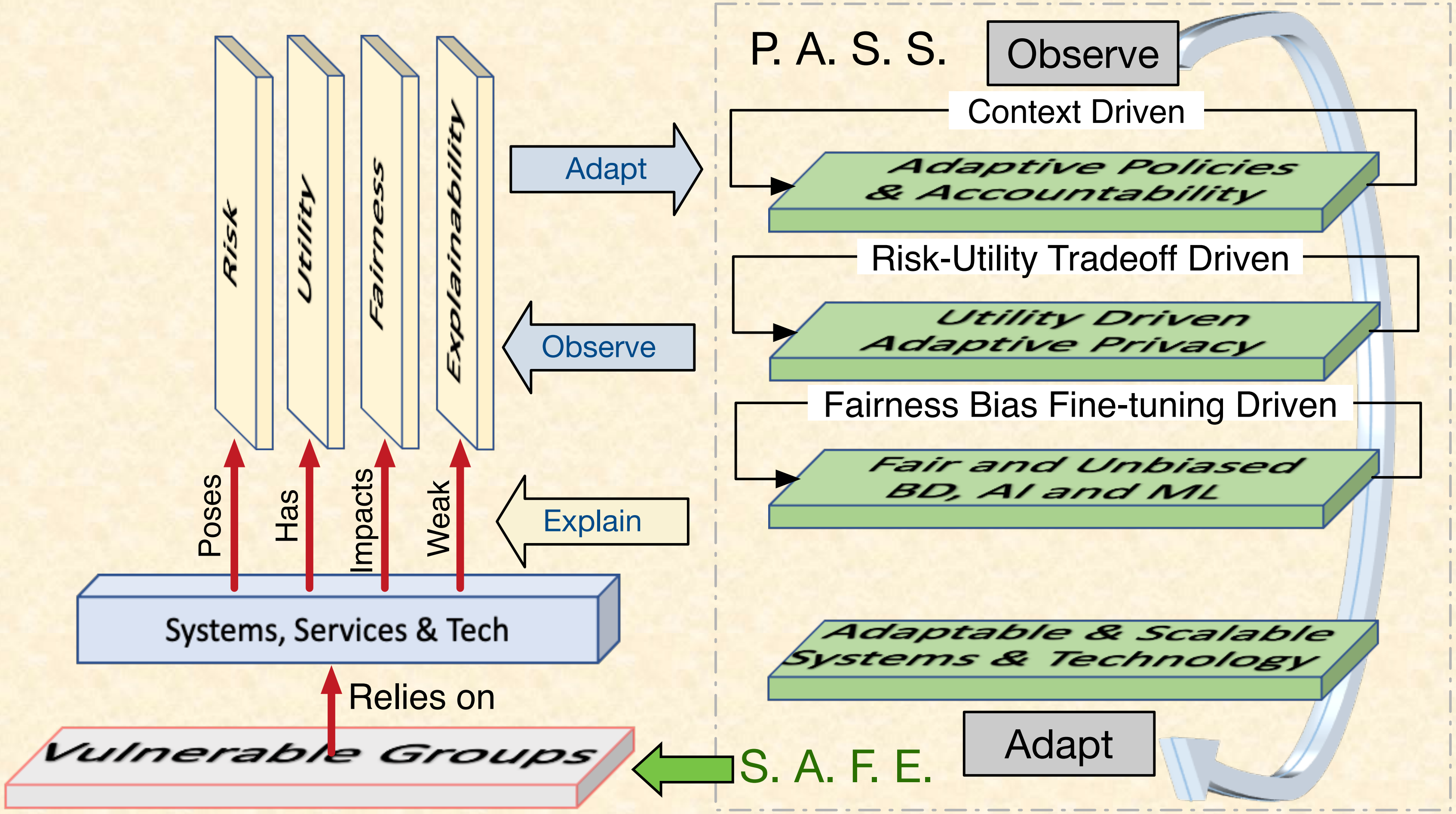
COLORADO STATE UNIVERSITY

What SAFE-PASS Hopes to Achieve



COLORADO STATE UNIVERSITY

SAFE-PASS Research Directions


Risk
Utility
Fairness
Explainability
Poses
Has
Impacts
Weak
Adapt
Observe
Explain
Systems, Services & Tech
Relies on
Vulnerable Groups
P. A. S. S.
Observe
Context Driven
Adaptive Policies & Accountability
Risk-Utility Tradeoff Driven
Utility Driven Adaptive Privacy
Fairness Bias Fine-tuning Driven
Fair and Unbiased BD, AI and ML
Adaptable & Scalable Systems & Technology
Adapt
S. A. F. E.

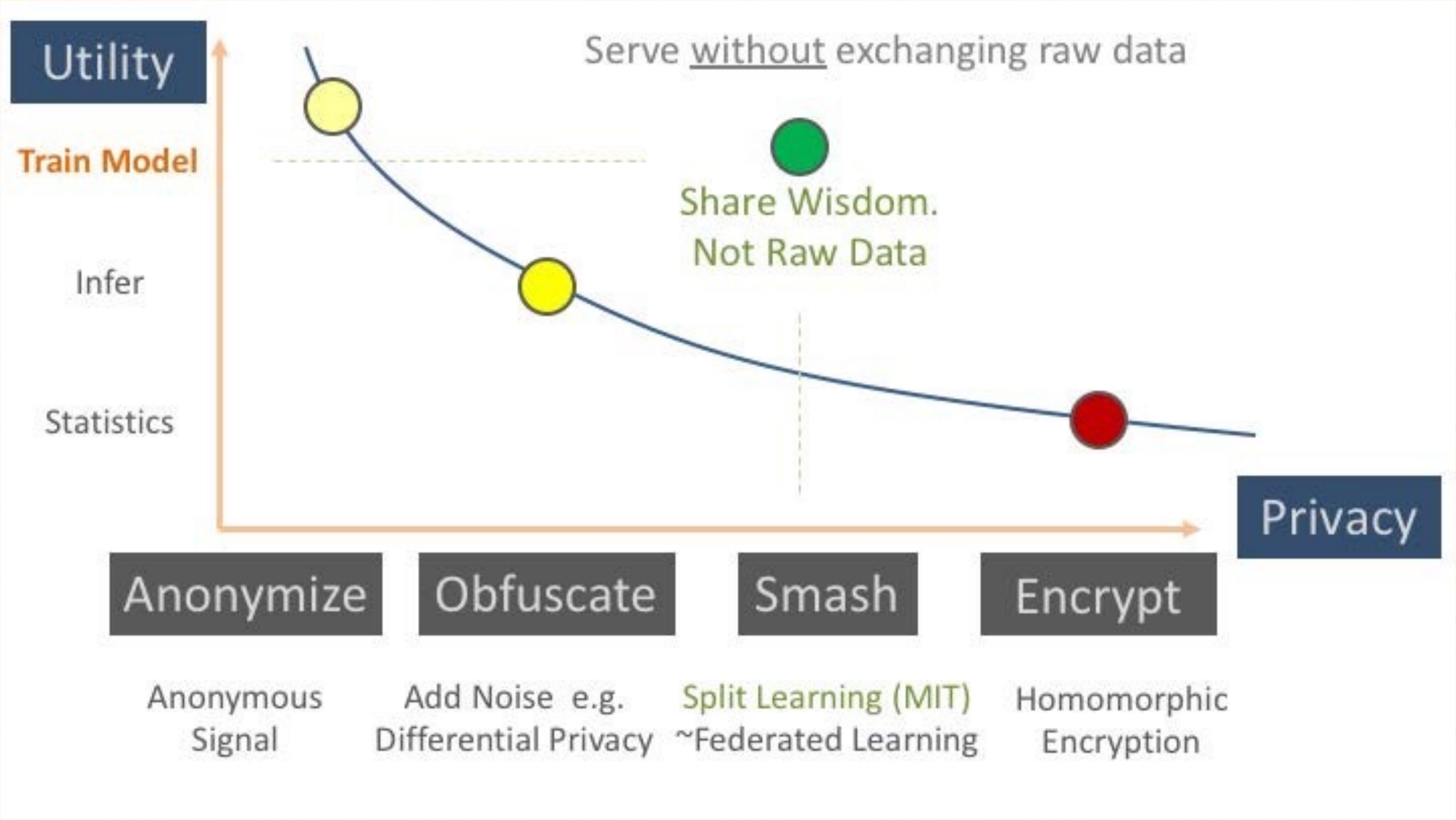
Adaptive Policies and Accountability

- Policy requirements elicitation via natural language statements
  - Security and privacy needs are context dependent
  - Multiple stakeholders impact policy needs of vulnerable groups
  - Need for constrained delegation
- Policy analysis
  - Conflicts between policies need to be removed
  - Consistency of policies with underlying rules and regulations
  - Potential abuse and attack on released data
- Policy evolution
  - Dynamic policies that change with changes in context

Utility Driven Adaptive Policies

- “Good to Share” policy (along lines of “Need to Know”)
  - How to determine when it is good to share
    - Utility of sharing vis-à-vis risk of sharing / utility of protecting
    - Utility is context dependent
- Situational awareness-based policy
  - Context-based authorization and access control
  - Context-based security
  - Context-based privacy

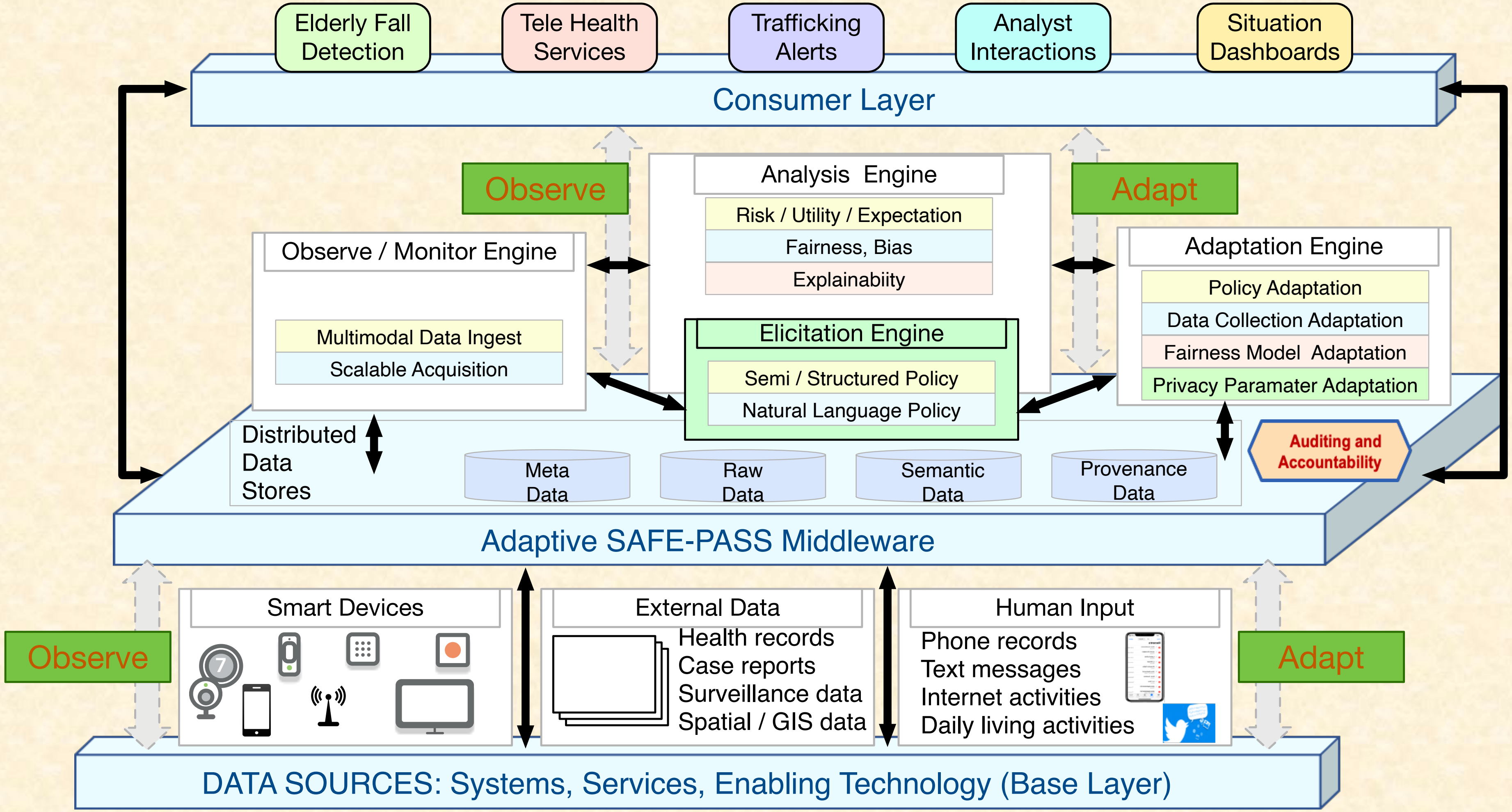
Utility vs Privacy Tradeoff



Fair and Unbiased Big Data, AI and ML

- Defining fairness in SAFE-PASS
  - Demographic aware fairness
    - All demographic groups are represented proportionally to the outcome or decision
  - Error aware fairness
    - Focus is on achieving similar error rates for diverse groups and the errors should be minimized
  - Impact aware fairness
    - Focus on long-term impact for different sub-populations
- Need to elicit information about the conception and reception of utility and fairness

SAFE-PASS Realization Architecture



Conclusions

- Vulnerable groups are more affected by security and privacy issues than non-vulnerable groups
    - Reluctant to share data
- Data sharing has benefits
- How to break the vicious cycle