



CCC

Computing Community Consortium
Catalyst

Towards a Privacy Research Roadmap for the Computing Community



EDITORS OF THE REPORT:
LORRIE CRANOR, TAL RABIN,
VITALY SHMATIKOV, SALIL VADHAN,
DANNY WEITZNER

Computing Community Consortium (CCC)



- Under CRA, funded by NSF
- The mission (CCC) is to:
 - catalyze** the computing research community and
 - enable** the pursuit of innovative, high-impact research
- CCC conducts activities that
 - strengthen** the research community,
 - articulate** compelling **research visions**, and
 - align** visions with pressing **national and global challenges**
- CCC **communicates** the importance of these visions to relevant parties (government, industry, academia)

Sources for the Report



- White House and PCAST Big Data Privacy Reports
- Responses to NITRD's RFI 9/2014
- NITRD workshop in February 2015
- Responses to CCC's request for contributions

Focus of our Report



- Privacy concerns raised by the:
 - Collection
 - Sharing
 - Analysis
 - Use
- of personal data in information systems

Why is Providing Privacy Difficult?

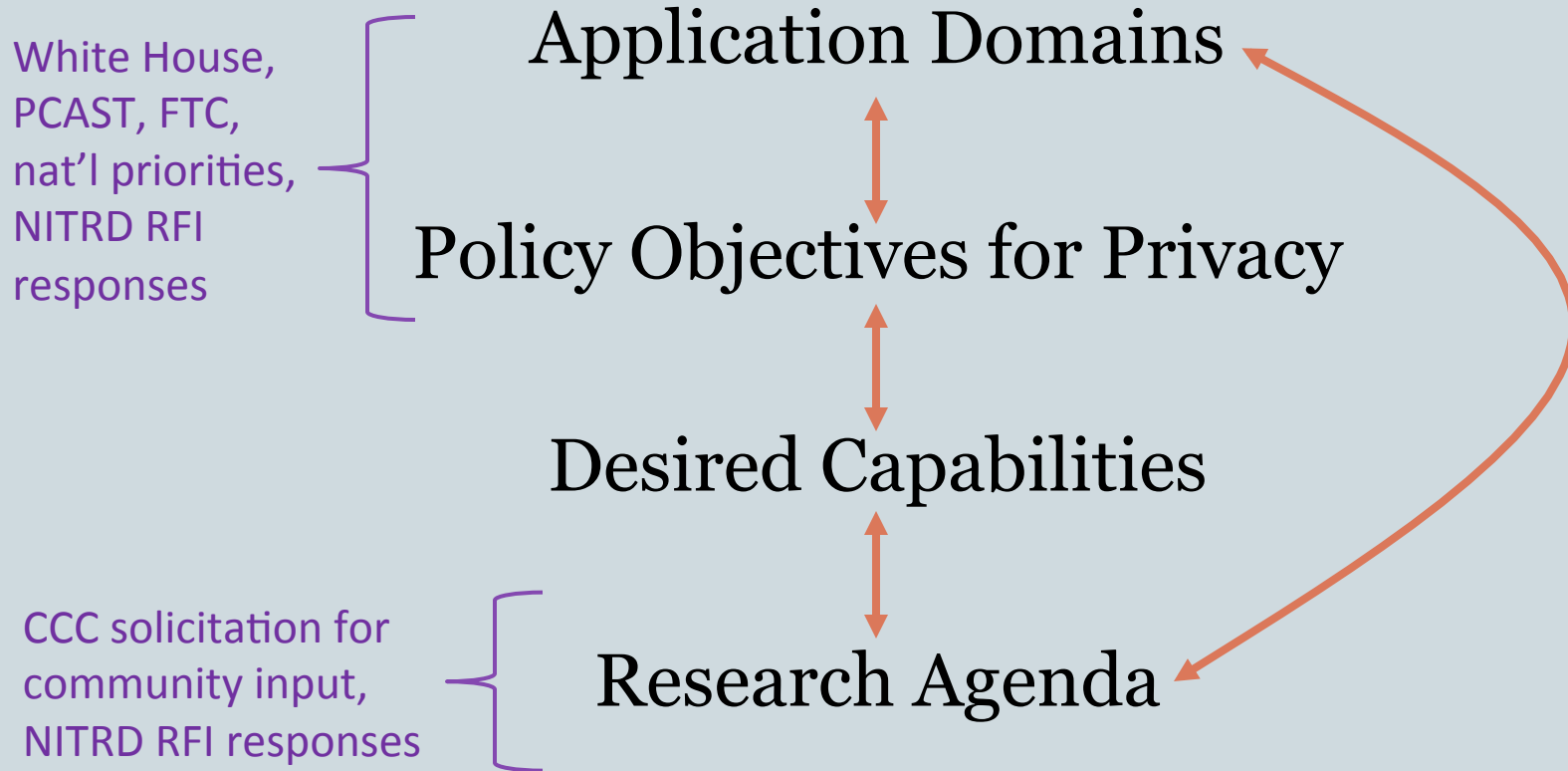


Tension between:

- Advances in computing and communication technology are bringing many benefits to society in such areas as: health care, transportation, national security, commerce
- Benefits involve use of sensitive personal data

Goal of research to balance the benefits with privacy rights and requirements of individuals

Deriving the Agenda



National Priorities & Application Domains



- Health Care
- Transportation
- Law Enforcement & National Security
- Education
- Modern Internet Services
- Modern App Ecosystems
- Internet of Things & Smart Infrastructures
- Financial Sector
- Open Government Data
- Research Data

Privacy Policy Objectives



- Data transparency
- Accountable information use
- Respect for context
- Individual control over personal data
- Privacy by design
- Access and correction to personal data
- Fairness
- Security

Desired Capabilities



- Measurement of Privacy
- Social Science of Privacy
- Security for Privacy
- Engineering of Privacy
- Policy for Privacy

Desired Capabilities



- **Measurement of Privacy**
be able to precisely define what various privacy objectives mean for different types of information systems, and be able to measure the extent to which the systems meet those objectives.
- **Social Science of Privacy**
- **Security for Privacy**
- **Engineering of Privacy**
- **Policy for Privacy**

Desired Capabilities



- **Measurement of Privacy**
- **Social Science of Privacy**
understand the privacy needs and expectations of the humans who use information systems, the institutional dynamics of the organizations that use personal data, and how larger social and economic forces relate to privacy.
- **Security for Privacy**
- **Engineering of Privacy**
- **Policy for Privacy**

Desired Capabilities



- Measurement of Privacy
- Social Science of Privacy
- Security for Privacy
understand the relationship between security and privacy, and be able to secure information systems from unauthorized access to personal info.
- Engineering of Privacy
- Policy for Privacy

Desired Capabilities



- Measurement of Privacy
- Social Science of Privacy
- Security for Privacy
- Engineering of Privacy
be able to design and build information systems that meet privacy objectives while allowing us to enjoy the beneficial uses of personal data.
- Policy for Privacy

Desired Capabilities



- Measurement of Privacy
- Social Science of Privacy
- Security for Privacy
- Engineering of Privacy
- Policy for Privacy
be able to design effective laws, regulations, policies, and best practices regarding the use of personal data in information systems in a way that recognizes the unique capabilities and limitations of information systems.

Research Directions



- Definitions and frameworks
- Measurements
- Algorithms, Statistics, and Machine Learning
- Cryptography
- Systems
- Usability and human behavior
- Economics
- Privacy and society

High-level Recommendations



- **A rigorous science of privacy:**
 - To defining and measure the privacy of information systems
 - Major challenge: not agreed upon definition of privacy (– can there be one?)
 - When examining a problem:
 - ✦ Precisely define the objective
 - ✦ Evaluate it with scientific rigor to prove whether the objective is met

High-level Recommendations (cont)



- Support the many stages and dimensions of privacy research:
 - Foundational work that aims to understand phenomena and the range of technological possibilities and limitations
 - Applied research that is directed at specific privacy objectives
 - Translational work that seeks practical impact on particular application domains.

High-level Recommendations (cont)



- **Priority to enable interdisciplinary research strategies:**
 - Developing a science of privacy and effective privacy solutions requires a combined understanding of computing technology, information, human behavior, and governance mechanisms

High-level Recommendations (cont)



- **Technology and policy dialogue:**
 - Multi-directional conversation that enables regulators, lawmakers, standards creators and system builders
 - To understand what is and is not possible to achieve with technology, and
 - Be informed of what should be integral privacy properties of systems, procedures and processes

Agenda Seeks to Lead to State Where:



Rigorous



that applies

over multiple domains

Agenda Seeks to Lead to State Where:



- Understand what people:

- Want



- Need



- And what we can give them

Agenda Seeks to Lead to State Where:

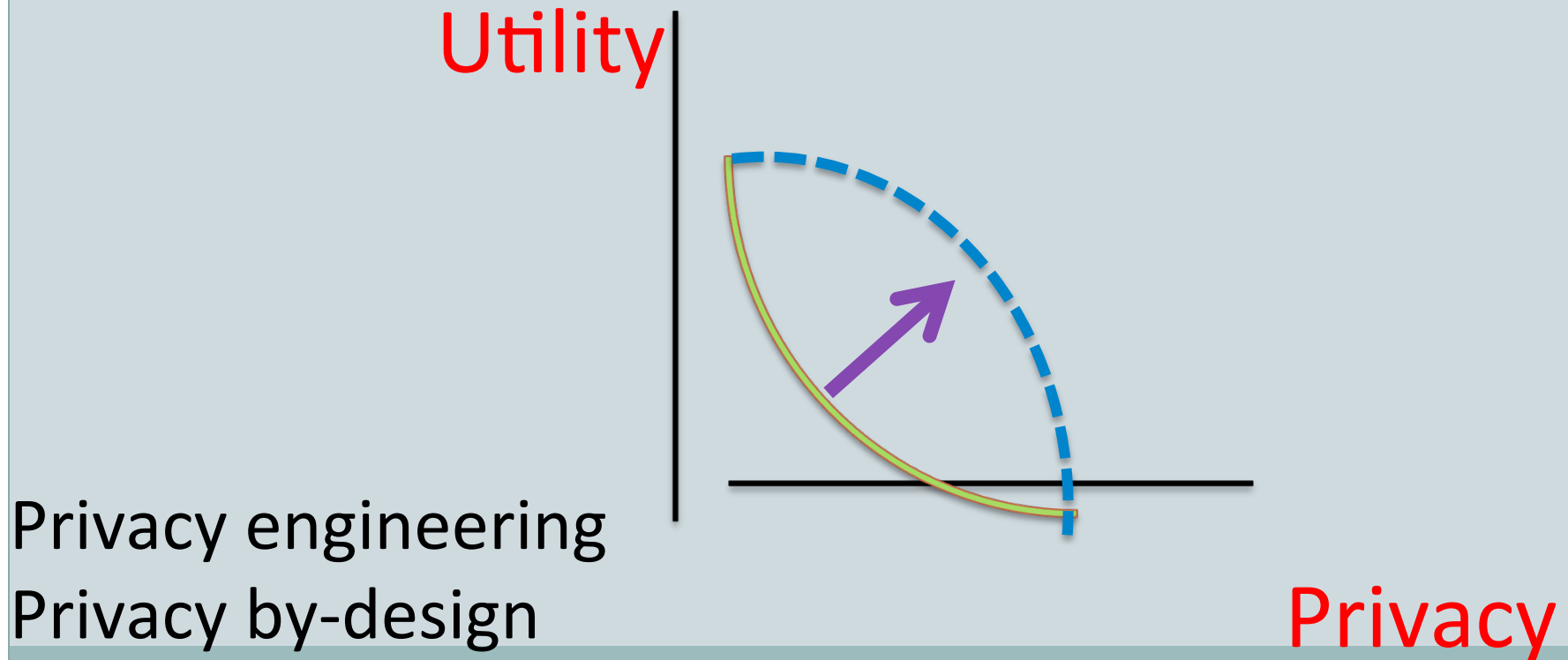


Recognizes the capabilities and limitations

Agenda Seeks to Lead to State Where:



- Systems can enable both privacy and the benefits of use of data to the maximum; showing we can achieve better tradeoff than we currently have



High-level Recommendations



- **A rigorous science of privacy:**
 - To defining and measure the privacy of information systems
 - Major challenge: not agreed upon definition of privacy (– can there be one?)
 - When examining a problem:
 - ✦ Precisely define the objective
 - ✦ Evaluate it with scientific rigor to prove whether the objective is met

High-level Recommendations (cont)



- Support the many stages and dimensions of privacy research:
 - Foundational work that aims to understand phenomena and the range of technological possibilities and limitations
 - Applied research that is directed at specific privacy objectives
 - Translational work that seeks practical impact on particular application domains.

High-level Recommendations (cont)



- **Priority to enable cross-disciplinary research strategies:**
 - Developing a science of privacy and effective privacy solutions requires a combined understanding of computing technology, information, human behavior, and governance mechanisms

High-level Recommendations (cont)



- **Technology and policy dialogue:**
 - Multi-directional conversation that enables regulators, lawmakers, standards creators and system builders
 - To understand what is and is not possible to achieve with technology, and
 - Be informed of what should be integral privacy properties of systems, procedures and processes

Health Care Domain



Benefits:

- more accurate diagnosis,
- more personalized and coordinated care,
- faster treatment development,
- better monitoring of patients through novel health tracking devices

Privacy concerns:

- disclosure of sensitive health data
- discrimination in employment or insurance based on medical conditions
- continual monitoring of patients outside the healthcare context through novel health-tracking devices

Transportation Domain



Benefits:

- reducing congestion
- preventing accidents; reducing deaths and injuries
- increasing fuel efficiency
- saving human effort spent on driving

Privacy concerns:

- tracking of individual movements through navigation systems, roadway sensors, traffic cameras, car data collection, and communications between cars

Internet of Things and Smart Infrastructures



Benefits:

- smart buildings, homes and cities
 - improve living conditions
 - enhances productivity and quality of life. E.g., a smart home can detect the occupant's presence, learn their schedules and requirements, and then combine that information with real-time utility prices and smart meters to provide efficient and automatic control of appliances

Privacy concerns:

- the same information can be used to
 - track when individuals are home
 - who they are
 - what TV programs they watch

Additional Domains



- Criminal Justice, Reconciling Privacy & Surveillance
- Education
- Internet Services (social networks, google, etc)
- Privacy Concerns in Modern App Ecosystems
- Financial Sector
- Open Government Data
- Research Data

Privacy Objectives and Desired Capabilities



- Measurement of privacy - enabling data transparency
- Social science of privacy
- Security for privacy
- Privacy-aware system building blocks - enabling privacy-by-design
- Policy of privacy (designing effective laws)

Research



- Definitions and frameworks
- Algorithms, statistics, machine learning, ...
- Systems: analysis, design, implementation, verification, auditing, communication
- Measurement
- Usability and human behavior
- Cryptography, MPC, search on encrypted data, ORAM,...
- Economics
- Privacy and society

Transition to Practice

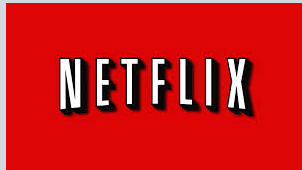


- Transition of privacy research to practice is critically important (and the most important goal)
- Involves several aspects:
 - engagement and education,
 - bridging the gap between research results and working, deployed products
 - creating funding models and structures that facilitate this transition

Where We Can (Possibly) Contribute




- Definitions – we have some success (MPC, differential privacy)
- Composition theorems



- Secure privacy enhancing protocols

Where We Can (Possibly) Contribute (cont)



- Security solutions that are tailored for privacy sensitive settings
 - Possibly paying a price in performance
- Measurements in unknown settings
 - Need to allow transparency to human or machine
-  Proprietary algorithms
- Speaking the language of privacy people

Why am I Talking about This Here?



- In addition to the obvious reasons
- Many European countries are in advanced stages of thought on the topic
- Would love to hear comments

Thank you!