Networking and Information Technology Research and Development Program

Federal Privacy R&D Priorities

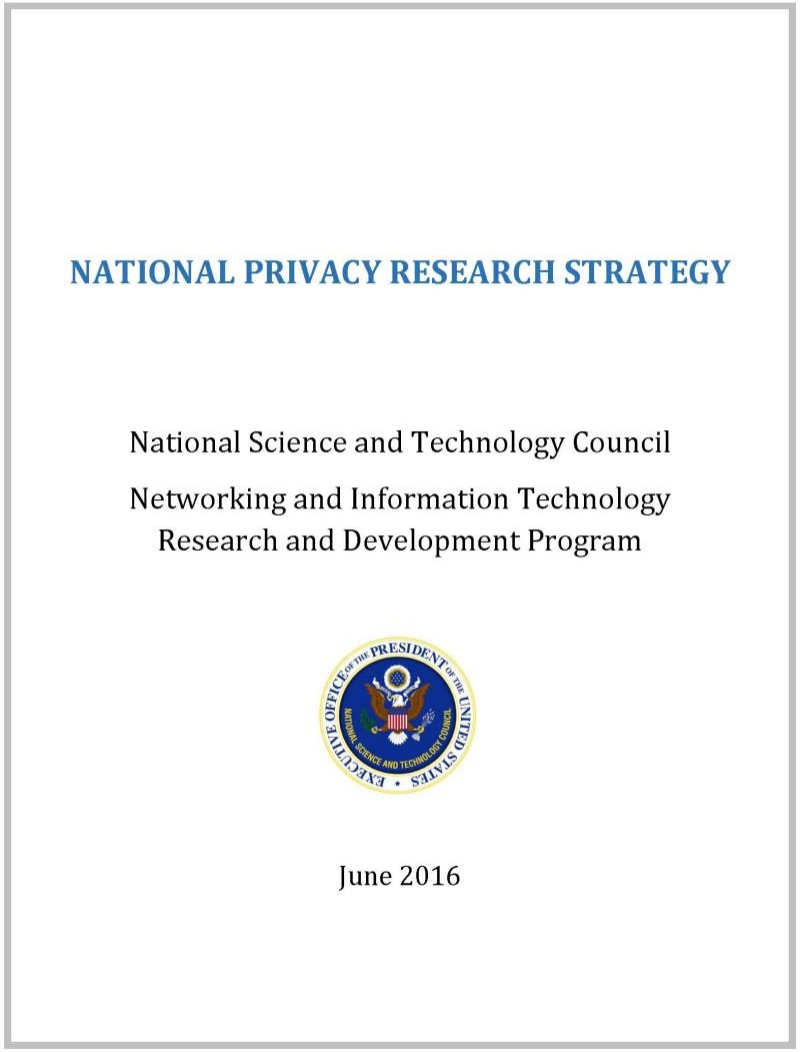
Science of Security Quarterly Meeting, Feb 2017

Tomas Vagoun
Cybersecurity and Privacy R&D Coordinator, NITRD

NITRD: Federal Networking and IT R&D (Program)

- Purpose
  - The primary mechanism by which the U.S. Government coordinates its unclassified Networking and IT R&D (NITRD) investments
  - Supports NIT-related policy making in the White House Office of Science and Technology Policy (OSTP)
  - Established in 1991
- Scope
  - Approximately $4.5 Billion/year across 18 agencies, 10 program areas
  - Cyber Security and Information Assurance (CSIA)
  - Enabling-R&D for High-Capability Computing Systems (EHCS)
  - High-Capability Computing Systems Infrastructure and Applications (HCSIA)
  - High Confidence Software and Systems (HCSS)
  - Human Computer Interaction and Information Management (HCI&IM)
  - Large-Scale Data Management and Analysis (LSDMA)
  - Large Scale Networking (LSN)
  - Robotics and Intelligent Systems (RIS)
  - Software Design and Productivity (SDP)
  - Social, Economic, and Workforce Implications of IT and IT Workforce Development (SEW)

For Today's Discussion



NATIONAL PRIVACY RESEARCH STRATEGY

National Science and Technology Council

Networking and Information Technology Research and Development Program

June 2016

https://www.nitrd.gov/PUBS/NationalPrivacyResearchStrategy.pdf

Background: White House & PCAST Recommendations

- President's Council of Advisors on Science and Technology (PCAST) Review of NITRD (2010)
  - Fed Gov. agencies should invest in a broad, multi-agency research program on the fundamentals of privacy protection and protected disclosure of confidential data
- PCAST Review of NITRD (2013)
  - Fed Gov. agencies should create a multi-agency collaborative effort to develop the scientific and engineering foundations of privacy R&D
- White House and PCAST Big Data and Privacy reports (2014)
  - Fed Gov. agencies should dramatically increase investment for R&D in privacy-enhancing technologies, encouraging cross-cutting research that involves not only computer science and mathematics, but also social science, communications and legal disciplines
- PCAST Review of NITRD (2015)
  - Federal Government should continue to develop and expand a multi-agency research and development program to advance the science, engineering, policy, and social understanding of privacy protection

Privacy … Historically

Privacy as solitude and confidentiality

- "Right to be let alone," Warren and Brandeis (1890)
- "Right of Privacy," Civil Law of New York State (1903), Abigail Roberson v. The Rochester Folding Box Company
- 1929 Census Act: disclosure of private information by Census Bureau agents punishable with imprisonment

Kodak camera, 1888
The National Museum of American History

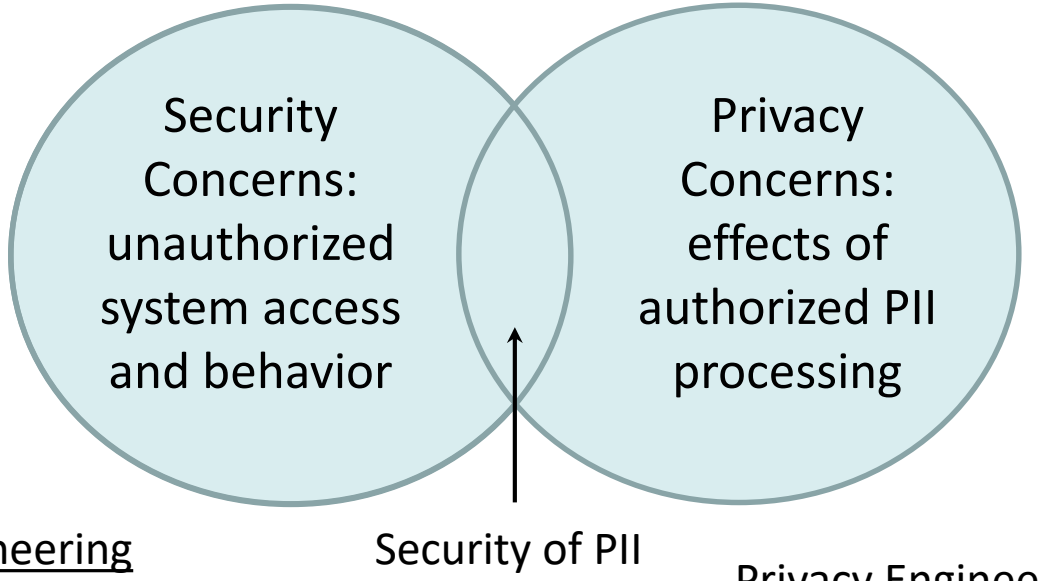
Abigail Roberson, 1902, sued to stop unauthorized use of her image

Privacy: What's Different Now?

- PCAST Big Data and Privacy report (2014): Privacy concerns arising from large-scale data collections , analysis and algorithmic decision making
  - Private facts inferred from fusion of non-sensitive data
  - Loss of anonymity from re-identification
  - Foreclosure of individual autonomy from biased or false conclusions and decisions by big data analytics
  - Violations of locational privacy and private association
  - No practical way to grant/decline consent for data collections in the world of sensors (e.g., IoT)
- White House Big Data report (2014)
  - Big Data is not neutral, BD analytics can endanger longstanding civil rights
- Privacy as personal autonomy
  - "Right to be forgotten," EU
  - FTC report on Data Brokers (2014): thousands of data segments on each US consumer
  - "Discrimination in Online Ad Delivery" (Sweeney 2013)

Information Security and Privacy

Security challenge: build systems that satisfy technical requirements



Privacy challenge: build systems that satisfy social requirements: privacy expectations (norms and laws)

<u>Security Engineering Objectives</u>

- Confidentiality
- Integrity
- Availability
- Nonrepudiation
- …

<u>Privacy Engineering Objectives</u>

- Predictability (contextual integrity)
- Disassociability (unlinkability)
- Manageability (intervenability)
- Transparency
- …
- [see NIST IR 8062/Privacy Engineering]

National Privacy Research Strategy

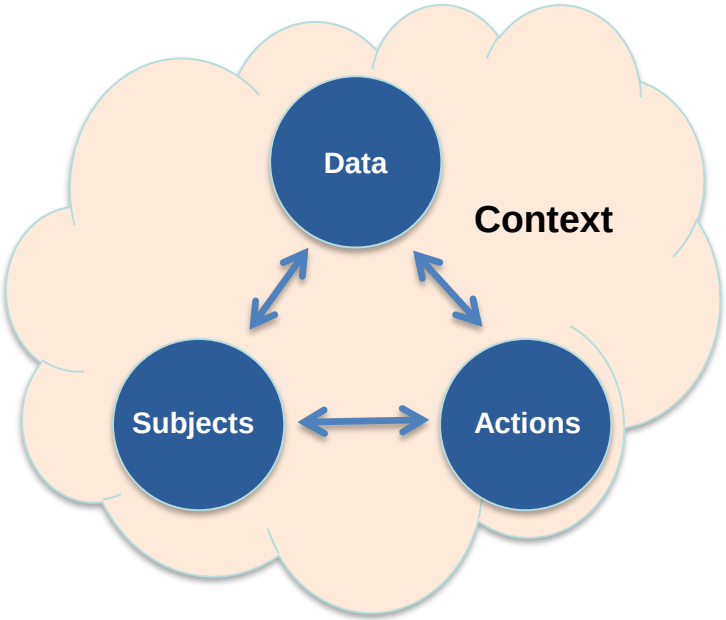
Key Privacy-related challenges:

- Privacy is Contextual
  - Privacy expectations and concerns vary by individuals, groups, and cultures, and are dependent on circumstances
- Lack of Transparency in Data Collection, Use, and Retention
  - Individuals have limited understanding and control of what data are collected about them, how they are used, and benefits gained from their use
- Increasing Data Aggregation, Analysis, and Release
  - Growing use of predictive algorithms that evaluate and score individuals; lack of understanding how individuals are affected
  - Growing concerns from the “mosaic effect” and re-identification of individuals

NITRD

Focus for Federal Privacy R&D

Privacy As



Role of Research

- Understand the nature of privacy
  - Privacy concerns solitude, confidentiality, the control of dissemination of personal information, the control of one's identity
  - Privacy is about the negotiation of personal spaces with those of peers, and with commercial and government entities
  - Privacy is contextual
- Understand privacy perspectives
  - Individual, Commerce, Government, Society
- Create knowledge and tools
  - To identify and mitigate emerging risks to privacy
  - To develop IT systems that can support privacy expectations and prevent unlawful discrimination, while supporting innovation

NITRD

Federal Priorities for Privacy Research

- Foster multidisciplinary approach to privacy research and solutions
- Understand and measure privacy desires and impacts
- Develop system design methods that incorporate privacy desires, requirements, and controls
- Increase transparency of data collection, sharing, use, and retention
- Assure that information flows and use are consistent with privacy rules
- Develop approaches for remediation and recovery
- Reduce privacy risks of analytical algorithms

NIST Privacy Engineering Program

NIST Privacy Engineering Goals

- Ability to design characteristics or properties of the system
- Support policy through mapping of system capabilities
- Support control mapping

NIST Privacy Engineering Objectives

- **Predictability**: enabling reliable assumptions by individuals, owners, and operators about personal information and its processing by an information system (contextual integrity)
- **Manageability**: providing the capability for granular administration of personal information including alteration, deletion, and selective disclosure
- **Disassociability**: enabling the processing of personal information or events without association to individuals or devices beyond the operational requirements of the system

DHS/CSD Data Privacy Program

DHS Privacy R&D Objectives

- Automating **control of personal data** to minimize cognitive overload and privacy risk
- Addressing **privacy concerns with connected devices, mobile computing**, and sensor platforms
- Addressing **privacy concerns with big data** and algorithms
- Managing **personally identifiable information** or information deemed sensitive while protecting individual privacy
- **Privacy respecting anomaly detection and counter-fraud technologies** with population scale applicability

DHS Privacy R&D Projects

- Differential Privacy for Anomaly Detection (DPAD)
  - Develop a framework of a privacy respecting screening capability to detect individuals, behaviors, areas, or data samples of high interest
- Privacy Preserving Federated Search and Sharing (PPFS2)
  - Addressing privacy concerns with big data and algorithms
- A Platform for Contextual Mobile Privacy
  - Develop a mobile phone based system to detect events deemed to be privacy sensitive by the user, and allow the user to make informed decisions on invoking specific privacy protections
- PriFi Networking for Tracking-Resistant Mobile Computing
  - Develop an anti-tracking and location-private network access mechanism (for WiFi and VPN)
- Applicability of Blockchain Technology to Privacy Respecting Identity Management
  - Data and application security at rest and in transit

NITRD

NIH and Privacy Research

National Institutes of Health (27 independent institutes)

- National Human Genome Research Institute
  - Impacts of privacy environments on personal health data, Genetic privacy, Harmonizing privacy laws, Privacy preserving technologies for human genome data
- National Institute of Biomedical Imaging and Bioengineering
  - Methods to enhance genomic privacy and data sharing, Encryption methods for privacy-preserving analysis of biomedical data, Privacy-protecting distributed analysis of biomedical big data
- National Library of Medicine
  - Protecting privacy of healthcare data in the cloud, Technologies to enable privacy in biomedical databanks
- Other institutes
  - Privacy perceptions and risks in molecular epidemiology, Data sharing and privacy protection in environmental health studies, Statistical health information release with differential privacy, Data anonymization
  - Obtaining consent in medical and healthcare settings

The Brandeis Vision

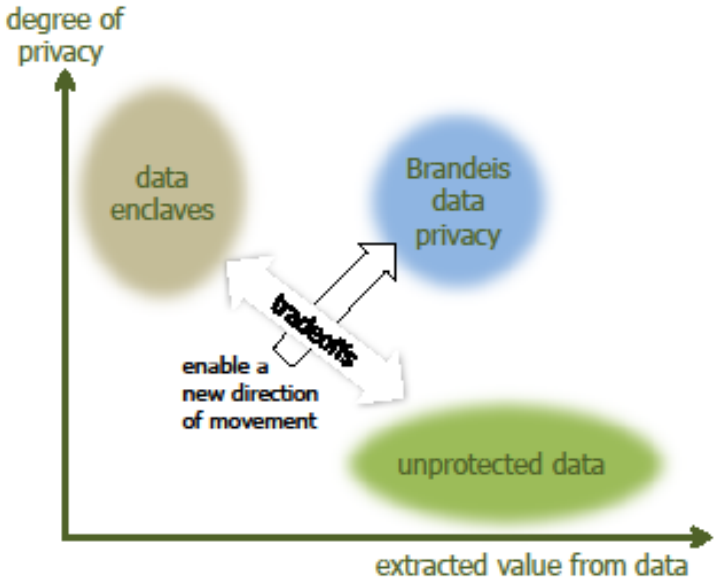
Vision

Break the tension between privacy and tapping the huge value of data

Goal

Learn how to build systems in which private data can only be used for the intended purpose and no other

- develop transferrable tools and techniques
- the data is protected against any other use



Potential for Impact

- Enable personal medicine, e.g. leveraging cross-linked genotype/phenotype data…
- Enable smart cities, e.g. smart buildings, smart energy use, smart traffic controls…
- Enable global data, e.g. every car sharing data on environment, weather, emergency situations…
- Enable internet awareness, e.g. every company and device sharing network and cyber-attack data…

… all without violating privacy

FTC Priorities for Privacy R&D

Federal Trade Commission's Needs for Research in Privacy

- Privacy-related notice and choice mechanisms
  - Evaluation methods and metrics
  - Approaches to making disclosures more effective
- Specific types of privacy-related disclosures
  - Effective disclosures in complicated multi-party ecosystem
  - Disclosures in an IoT world
  - Algorithmic transparency – what do users want to know and how can it be conveyed effectively?
- Understanding and quantifying privacy and security
  - Valuation of privacy
  - Impact of information exposure and analysis
  - Balancing privacy interests with other interests
- Consumer and business education
  - How to evaluate behavior change through educational intervention?
  - What approaches to educational intervention are most effective?
- Tools and techniques
  - Help control personal info
  - Detect data collection and sharing, online tracking, cross-device tracking
  - Detect discrimination in algorithms
  - Quantify security & privacy risks
  - Evaluate content and meaning of privacy policies

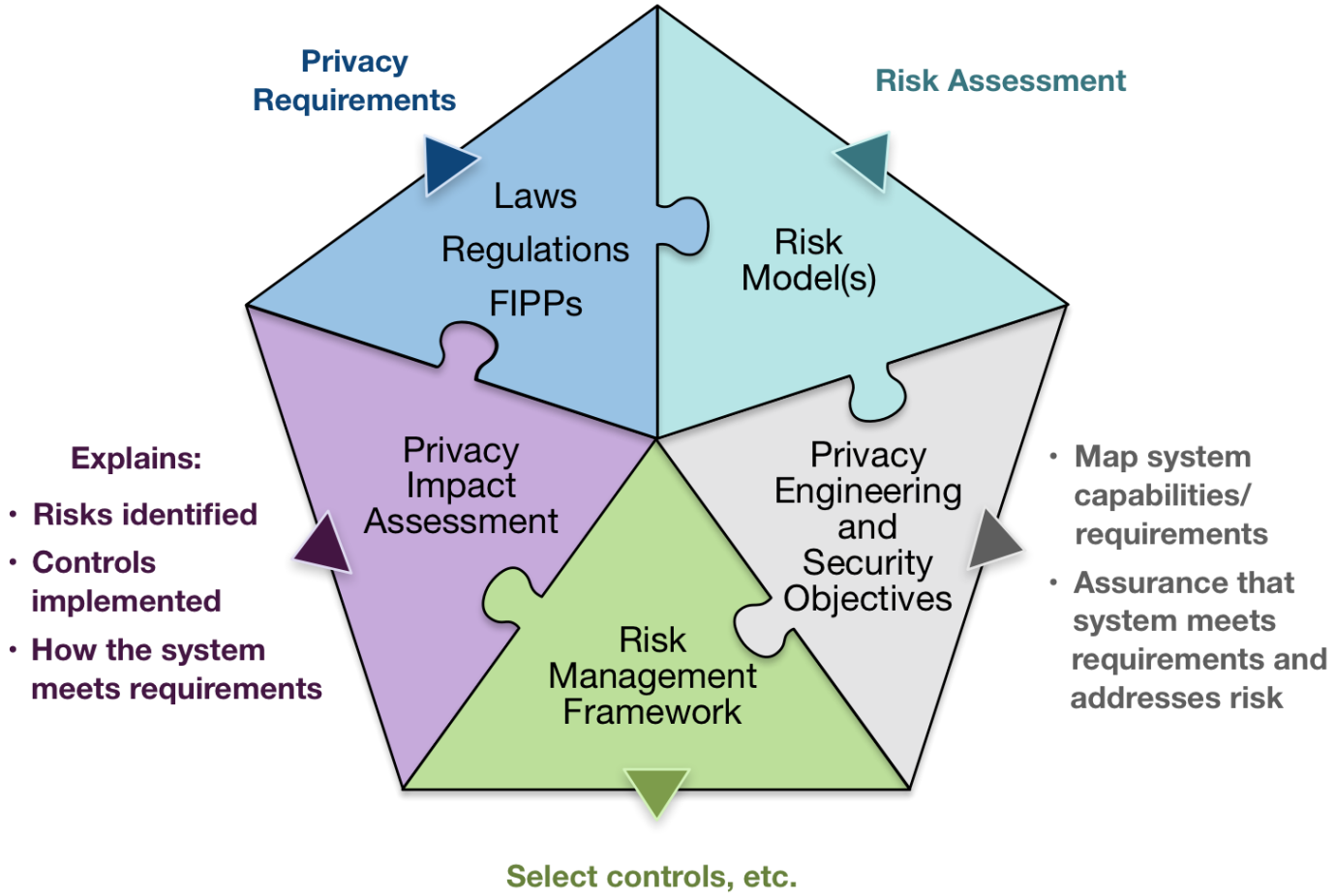
NSF

NSF SaTC PI Survey (Jan 2017)

"select all topics that describe your projects"

NPRS Privacy Research Priorities (1278 responses)		
Does Not Apply	252	20%
Foster multidisciplinary approach to privacy research and solutions	212	17%
Understand and measure privacy desires and impacts	148	12%
Develop system design methods that incorporate privacy desires, requirements, and controls	269	21%
Assure that information flows/use are consistent with privacy rules	144	11%
Increase transparency of data collection, sharing, use, and retention	103	8%
Reduce privacy risks of analytical algorithms	79	6%
Develop approaches for remediation and recovery	71	6%

Putting It All Together



For More Information

Tomas Vagoun, PhD
Cybersecurity and Privacy R&D Technical Coordinator
National Coordination Office for NITRD
vagoun@nitrd.gov