NITRD
National Privacy Research Strategy
Introduction

Tomas Vagoun
NCO/NITRD
vagoun@nitrd.gov
2/5/15


The Office of the National Coordinator for
Health Information Technology


U.S. DEPARTMENT OF HOMELAND SECURITY


NSF


NNSA
National Nuclear Security Administration


DARPA


NIST
National Institute of
Standards and Technology


NATIONAL INSTITUTES OF HEALTH


NOAA
NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION
U.S. DEPARTMENT OF COMMERCE

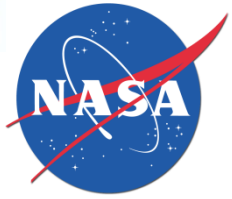

NITRD

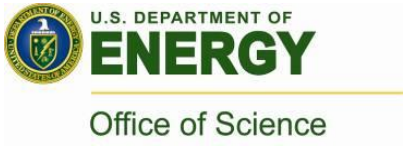

UNITED STATES
ENVIRONMENTAL PROTECTION AGENCY


DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA


NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA


NATIONAL
ARCHIVES


NASA


U.S. DEPARTMENT OF
ENERGY
Office of Science


NATIONAL RECONNAISSANCE OFFICE
UNITED STATES OF AMERICA


AHRQ

NITRD (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)
- Scope
  - Approximately $4B/year across 16 agencies, seven program areas
  - Cyber Security and Information Assurance (CSIA)
  - Human Computer Interaction and Information Management (HCI&IM)
  - High Confidence Software and Systems (HCSS)
  - High End Computing (HEC)
  - Large Scale Networking (LSN)
  - Software Design and Productivity (SDP)
  - Social, Economic, and Workforce Implications of IT and IT Workforce Development (SEW)
  - Established by the High-Performance Computing Act of 1991

Policy Context, Examples

- Big Data: Seizing Opportunities, Preserving Values, The White House, May 2014
  - "must ensure the big data analytics are used in ways that protect the public as well as the civil liberties and privacy rights"
- EO 13642: Making Open and Machine Readable the New Default for Government Information, WH, May 2013
  - "agencies shall ensure that they safeguard individual privacy, confidentiality, and national security;" "agencies shall incorporate a full analysis of privacy, confidentiality, and security risks"
- EO 13636: Improving Critical Infrastructure Cybersecurity, WH, Feb 2013
  - "ensure that privacy and civil liberties protections are incorporated;" "such protections shall be based upon the Fair Information Practice Principles"

Policy Context (2)

- PPD 21: Critical Infrastructure Security and Resilience, WH, Feb 2013
  - "information sharing within the government and with the private sector must be done while respecting privacy and civil liberties"
- Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Consumers, FTC, Mar 2012
  - Privacy by Design; consumers to be able to make decisions about the use of private data; greater transparency for information collection and use practices
- Consumer Data Privacy in a Networked World: a Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, WH, Feb 2012
  - Consumer Privacy Bill of Rights, expanding FIPPs to cyberspace: Individual Control, Transparency, Respect for Context, Security, Access and Accuracy, Focused Collection, Accountability

Policy Context (3)

- U.S. International Strategy for Cyberspace, WH, May 2011
  - "individuals should be able to understand how their personal data may be used, and be confident that it will be handled fairly"
- The National Strategy for Trusted Identities in Cyberspace (NSTIC), WH, Apr 2011
  - "The Identity Ecosystem Framework must offer individuals better means of protecting their privacy … based upon the FIPPs"

Policy Context (4)

- Commercial Data Privacy and Innovation in the Internet Economy: Dynamic Policy Framework, DOC, Dec 2010
  - "advancing consumer privacy through a focus on transparency, purpose specification, use limitation, and auditing;" "maintaining dynamic privacy protections through voluntary, enforceable, FTC-approved codes of conduct"
- Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, WH , May 2009
  - "the government must protect privacy rights;" "build an identity management strategy that addresses privacy and civil liberties, leveraging privacy-enhancing technologies"

PCAST Recommendations

- Big Data and Privacy: a Technological Perspective, PCAST, May 2014
  - Technological foundation for privacy: move from the focus on controlling the collection and storage of personal data to controlling the use of the data and data derived from analytics
- PCAST reports on the NITRD Program, Jan 2013 and Dec 2010
  - Fed Gov to create a broad multi-agency collaborative effort to develop the scientific and engineering foundations of privacy R&D, and the fundamentals of privacy protection and protected disclosure of confidential data

US Congress

- Cybersecurity Enhancement Act of 2014: on Federal cybersecurity R&D objectives
  - “How to guarantee the privacy of an individual, including that individual’s identity, information, and lawful transactions when stored in distributed systems or transmitted over networks”

NPRS Objectives

- OSTP request to NITRD: prepare a draft National (Federal) Privacy Research Strategy (NPRS)
- NPRS shall
  - Establish objectives and prioritization guidance for Federally-funded privacy research
  - Provide a framework for coordinating R&D in privacy-enhancing technologies
  - Encourage multi-disciplinary research that recognizes the needs of the Government, the needs of the society, and enhances opportunities for innovation in the digital realm

Understanding Privacy

- Government Perspective
  - Execute laws, find ways to support privacy requirements of such laws, law enforcement, national defense
  - Creating laws/regulations affecting privacy
- Individual Perspective
  - Concerns about the collection and control of personal data that is collected and how it is used
- Commerce Perspective
  - Pursuit of business opportunities that involve collection and use of personal information, in marketing, big data analytics, etc.
- Society Perspective
  - Concerns about effects from the loss of privacy on society as a whole, such as erosion of freedom, self-censoring, compartmentalization of people in cyberspace, informational discrimination, etc.
  - How to balance IT innovation with privacy protection

Privacy in the Real World

- One of the ways to think about privacy are concerns about people's ability to avoid harm by being aware of and able to manage what personal information is disclosed, to whom, when, under what circumstances, and for what purposes
- Social and institutional structures create context
- An individual is a member of circles/groups with their own norms

Privacy Groups

- Groups
  - Social (family, friends, etc.), Professional (employment, medical, etc.), Commerce (on-line retail transactions), Government, etc.
  - Groups have different norms/expectations/rules for what is acceptable
  - Group norms may be dynamic
- Violation of privacy
  - Deviations from the norms of a particular group
  - A result of a difference of norms across multiple groups
- Controls
  - Different groups can have varying controls of information flows/disclosures
- ➢ The social/sociological view of privacy (privacy groups, context) facilitates a natural understanding of privacy

Notional Privacy Research Framework

- Social/sociological privacy model and constructs provide a framework to describe privacy and where research contributions fit
- Research in privacy should lead the way toward the realization of sociological privacy constructs in cyberspace
- Research themes should identify key gaps in our abilities to realize desired sociological privacy constructs (objects, rules, interactions, controls, etc.) in cyberspace

For More Information

Tomas Vagoun, PhD
Cybersecurity R&D Technical Coordinator

National Coordination Office for
Networking and Information Technology Research and Development
Suite II-405, 4201 Wilson Blvd.
Arlington, VA 22230
Tel: (703) 292-4873
vagoun@nitrd.gov

http://www.nitrd.gov