Federal Networking and Information Technology
Research and Development Program

Report on Privacy Research within NITRD

National Coordination Office for NITRD
April 23, 2014

Table of Contents

Summary 3

Privacy Research within NITRD 5

- OSTP Request For Information 5
- Privacy Research Characterization 6
- Privacy R&D Strategy 7
- Privacy Research Activities within NITRD 9
- Summary 17

Comments and Next Steps 18

Summary

The President's Council of Advisors on Science and Technology (PCAST) 2013[1] and 2010[2] reviews of the Federal Networking and Information Technology Research and Development (NITRD) Program[3] have identified challenges to personal privacy in the digital era as a significant impairment undermining societal benefits from large-scale deployments of networking and IT (NIT) systems. Consequently, PCAST has called upon federal research agencies to create a multi-agency initiative focused on developing scientific and engineering foundations for protecting privacy, which could then be the basis for new technologies and solutions in this space.

In August 2013 and in February 2014, the White House Office of Science and Technology Policy (OSTP) issued two Requests For Information (RFI) to NITRD on privacy research activities pursued by the agencies in NITRD, to understand what research is taking place, and to explore a possible multi-agency research agenda in foundations of privacy. This report summarizes current research in privacy within NITRD. The responses indicate that agencies are funding a broad range of R&D relevant to privacy, across four areas:

- Supporting privacy as an extension of security
- Characterizing privacy objectives and establishing compliance regimes and methods
- Assuring privacy in healthcare in compliance with healthcare privacy laws
- Exploring basic privacy constructs and their application in many areas of NIT

Funding estimate

Responses provided by agencies indicate that approximately $77M per year is invested in privacy research activities across NITRD:

Research areas	Support for privacy as an extension of security	Privacy characterization and compliance	Privacy in healthcare	Privacy research explorations
Agencies	AFRL, DARPA, NSA, IARPA, ONR	DOE, DHS, NIST	TATRC, ONC, NIH	NSF
Funding estimate Total of $77M/year	$34M/year	$10M/year	$8M/year	$25M/year

[1] "Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology," January 2013, http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-nitrd2013.pdf

[2] "Designing a Digital Future: Federally Funded Research and Development Networking and Information Technology," December 2010, http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-nitrd-report-2010.pdf

[3] Networking and Information Technology Research and Development (NITRD) Program provides a framework in which many US Government agencies come together to coordinate networking and information technology research and development efforts. More information is available at http://www.nitrd.gov

Note: funding estimates are subject to revision, should additional information become available.

Explicit vs. derived privacy research

Research relevant to privacy challenges in NIT includes activities initiated with privacy research as the predominant objective as well as activities where benefits to privacy are secondary or derived outcomes. Based on the provided responses, a large portion of research in privacy within NITRD is undertaken with explicit privacy objectives:

	Explicit privacy research	Derived privacy research
Agencies	DHS, DOE, IARPA, NIH, NIST, NSF ($11M/year), TATRC, ONC	AFRL, DARPA, NSA, NSF ($14M/year), ONR
Funding estimate	$49M/year	$28M/year

Privacy R&D strategy

Agency responses indicate that current privacy research efforts are driven by the needs and missions of individual agencies and are not coordinated by multi-agency strategic plans or frameworks. Furthermore, agencies do not cite any coordinated efforts specifically focused on developing scientific and engineering foundations for privacy in NIT.

While there are many innovative research projects within NITRD addressing a broad range of privacy challenges in cyberspace, no overall strategy has been reported that would unite topical interests among the agencies and serve as the basis for coordinated R&D in this area. Agencies would likely benefit from initiatives that could bring together computer and information scientists with social, behavioral, and economic scientists and with public and private stakeholders to both identify a robust multi-agency research and development agenda and the capabilities and technologies that would have leverage in both physical and cyber space.

This report was prepared by the National Coordination Office for NITRD. Electronic versions of NCO/NITRD documents are available on the NCO website: http://www.nitrd.gov.

Questions or comments about this report can be directed to:
Tomas Vagoun
NCO Cybersecurity R&D Technical Coordinator
vagoun@nitrd.gov

Privacy Research within NITRD

OSTP Request For Information

In August 2013 and February 2014, OSTP asked NITRD agencies to respond to the following questions:

1. Provide a description of your criteria used to determine whether your agency's activity or program is or contributes significantly to "privacy research"
2. For each identified current or planned R&D activity or program in privacy research provide: (a) name of the activity or program, (b) summary of the activity or program, (c) approximate funding or level-of-effort for the activity or program, (d) describe what privacy requirements or objectives are being addressed, (e) describe the privacy research work being performed, (f) discuss whether the R&D activity has been (or will be) initiated with privacy research as its main (or predominant) objective, or whether the activity is predominantly research in other areas, such as security, with its application to privacy as a by-product, (g) discuss any international efforts in privacy policy and privacy technology research.
3. Provide a summary of prior R&D activities or programs in your agency/office that have contributed significantly to privacy research
4. Provide pointers to any relevant federal R&D activities outside the NITRD program
5. Discuss key privacy-enabling capabilities or technologies that would benefit from coordinated, multi-agency R&D efforts

Responses

The following agencies responded to the RFIs:

- Air Force Research Laboratory (AFRL)
- Army / Research and Technology
- Department of Defense / Defense Advanced Research Projects Agency (DARPA)
- Department of Defense / Office of Secretary of Defense (OSD)
- Department of Defense / Telemedicine and Advanced Technology Research Center (TATRC)
- Department of Education
- Department of Energy / Office of Electricity Delivery and Energy Reliability (DOE/OE)
- Department of Health and Human Services / Office of the National Coordinator (ONC)
- Department of Homeland Security / S&T Cyber Security Division (DHS)
- National Aeronautics and Space Administration (NASA)
- National Institute of Standards and Technology / Information Technology Laboratory (NIST) & NIST / National Strategy for Trusted Identities in Cyberspace (NIST/NSTIC)

- National Institutes of Health / National Cancer Institute (NIH/NCI)
- National Institutes of Health / National Institute of General Medical Sciences (NIH/NIGMS)
- National Institutes of Health / National Library of Medicine (NIH/NLM)
- National Science Foundation (NSF)
- National Security Agency / Research Directorate (NSA)
- Office of the Director of National Intelligence / Intelligence Advanced Research Projects Activity (IARPA)
- Office of Naval Research & Navy Research Laboratory (ONR)

Agency responses were collected by the NCO and are summarized in the following sections.

Privacy Research Characterization

In order to better understand what privacy research is being conducted by the agencies, the survey deliberately did not define or characterize what would constitute as "privacy research." Agencies were asked to provide their definitions of privacy research. The responses included:

Agency	**Criteria used to determine whether an activity is privacy research**
AFRL	S&T that addresses the control, management, access restriction, and use of individual's personal information and identity verification.
DARPA	Research that supports confidentiality in computation and communication contributes significantly to "privacy research".
OSD	For DoD Cyber S&T activity to be "privacy research" it must support one or more of the Fair Information Practice Principles identified in the Consumer Privacy Bill of Rights: Individual Control, Transparency, Respect for Context, Security, Access and Accuracy, Focused Collection, Accountability.
DHS	Support R&D aimed at improving privacy protection capabilities; Produce innovative privacy-enhancing solutions that embed privacy controls while addressing mission requirements (e.g., reduce the time, improve the accuracy and automate the information review, assessment, and tagging of data/information for privacy compliance); Support the need of individual citizen privacy while furthering security interests.
NIH/NCI	Activity contributes to NCI's research in statistical confidentiality of cancer registry data. For example: 1) evaluating the of risk of disclosing the identities of cancer patients in a cancer registry database, 2) developing statistical methods to synthesize certain data values in a cancer registry database to minimize the risk of disclosure, while maintaining the statistical utility of the data.
NIH/NIGMS	Privacy research within NIGMS is conducted through investigator initiated project research grants, executed under the National Centers for Biomedical Computing.
NIH/NLM	NLM does not have an extramural initiative devoted solely to privacy research, but has funded privacy-related research for more than a decade, in biomedical informatics,

	including clinical informatics, public health informatics, translational bioinformatics and consumer informatics.
NSF	NSF activities are driven bottom-up by research proposals from the academic research community. Hence, contribution to privacy research is primarily determined by the research community's view of the field.
NSA	Criteria for "privacy research" are research into new algorithms and techniques that have privacy protection as a primary or major application.
ONR	Research that enhances anonymity of activities in cyber-world; Research that prevents/reduces leak of private and personally identifiable information at end devices; Research that develops mechanism & policy to enhances protection on private information in collaborative query-able environment.

Privacy R&D Strategy

The survey solicited agency inputs on privacy-enabling capabilities, technologies, and research strategies. The responses included:

AFRL: Federally-funded and other coordinated multi-agency R&D would benefit privacy research in areas where personally-identifiable information requires protection against threats that exceed the capabilities of commercially available privacy solutions.

ONC: The following topics would benefit from additional research: (a) educating individuals about privacy and how to effectively communicate privacy notice information to individuals in a manner that they can readily understand, (b) how to correctly identify patients across healthcare settings while maintaining the privacy rights of patients, data integrity, accuracy and security of patient health information, (c) managing patient consent rights with respect to the electronic exchange of their health information, (d) developing standards that will allow patients and providers to perform data segmentation.

NIST: Federally-funded R&D could make a positive contribution to privacy solutions that help to manage monitoring, tracking, information sharing, and data analysis.

NSF: A Privacy Leap-Ahead Initiative (modelled after the 2009 OSTP/NITRD Cyber Leap Year Initiative) could bring together computer and information scientists with social, behavioral and economic scientists and with public and private stakeholders to identify a multi-agency robust research and development agenda.

IARPA: The ability to conduct business, social, or interpersonal transactions without risk of unnecessarily disclosing private information is a key enabler of freedoms of speech, religion, association, and the press. The ability to control dissemination of personal data for purposes other than that for which it was originally provided is also fundamental to privacy. Federal R&D can make a positive contribution by investing in fundamental research that promotes these abilities.

IARPA: Multiparty computation (MPC) will become a ubiquitous computing paradigm as the use of personal information becomes more and more widespread, becomes monetized, and access to data becomes abstracted from its geographical location. Commercial data storage providers offer data access services while locating the physical storage media almost anywhere in the world, and replicating or moving the data seamlessly and transparently to the service users. This means that risks to security and privacy based on physical access to storage media will become very difficult to assess, at the same time that the need for privacy protections is growing. MPC will provide assurance that data is secure in spite of physical access.

ONR: Additional research is needed in the areas of: (a) device fingerprinting: in addition to network metadata, communication devices are subject to fingerprinting and tracking by adversaries—understanding both fingerprinting techniques and countermeasures is therefore important, (b) practical applications of membership-concealing networks: developing practical techniques to permit communication over shared or public networks that conceal the participation in a private and secure subnet.

Privacy Research Activities within NITRD

This section summarizes current research activities by NITRD agencies related to privacy.

Agency	Activity Name	Activity Summary	Privacy Objectives
AFRL	Secure Sensor Semantic Web and Information Fusion Project duration: 2009-2011	Developing data management techniques for managing sensor databases.	Access restriction, anonymity, security policy integration
AFRL	PREDICT Privacy and Security Enhancing Dynamic Information Monitoring with Feedback Guidance Project duration: 2012-2014	Develop new mechanisms and capabilities to support privacy enhancing dynamic data monitoring.	Access restriction, anonymity, privacy preserving data aggregation
AFRL	Comprehensive Toolset for General-Purpose Private Computing and Outsourcing Project duration: 2013-2015	Techniques to permit general-purpose computing on sensitive data in multi-party and outsourced contexts.	Access restriction, anonymity
DARPA	PROgramming Computation on EncryptEd Data (PROCEED) Project duration: FY2011-14	Develop methods to enhance the security of cloud computing by enabling computing with encrypted data without first decrypting it.	Confidentiality of computation Secure multiparty computation
DARPA	Safer Warfighter Communications (SAFER)	Develop technologies for assured and trustworthy Internet communications in untrusted and adversarial environments.	Confidentiality of Internet-based communication
TATRC	EHR/Privacy Standards and Agile Development Research and Support	Identify data integration processes related to patient privacy and identity management to support the development of a joint VA–DoD EHR.	Patient privacy, patient consent and identity matching

TATRC	NwHIN Patient Consent Repository and HHS Pilot	Identify requirements and perform gap analysis of HIT standards required for Patient Consent Directive (PCD) exchange.	Dynamic review of PHI requests from a PCD repository
TATRC	Policy Issues for Health Information Technology and Health Informatics	Design of the research roadmap for patient privacy.	Patient privacy policies
TATRC	Open Enterprise Master Patient Index	Develop deterministic and probabilistic record matching algorithms.	Patient data quality in National Health Information Exchanges
TATRC	RESTful Health Exchange (RHEx) for Exchange Diagnostic Images	Develop a prototype to demonstrate the secure exchange of diagnostic images between network radiologist and MHS providers	Security of patient health records
DOE/OE	Privacy Voluntary Code of Conduct (VCC)	Develop a Voluntary Code of Conduct (VCC) for utilities and third parties providing consumer energy use services.	Protecting the access, use, and sharing of customers' electricity usage and related data
ONC	Strategic Healthcare Information Technology Advanced Research Projects on Security (SHARPS) Grant Program Program end: March 2014	SHARPS is a multi-institutional and multi-disciplinary research project, with the goal to investigate ways to develop security functions, policies and technology that will facilitate increasingly widespread, rapid and sophisticated, electronic use and exchange of health information while assuring individuals' safety and privacy.	Requirements, foundations, design, development, and deployment of security and privacy tools and methods for electronic use and exchange of health information
ONC	Data Segmentation Project	Data Segmentation for Privacy: the process of sequestering from capture, access or view certain data elements that are perceived by a legal entity, institution, or individual as being undesirable to share.	Use Limitation and Collection Limitation; Metadata standards that enable segmentation required by varying disclosure policies
ONC	Data Provenance Project	Explore the use of metadata to indicate the "provenance" (original source) of health information in an electronic health record.	Data quality in EHR

ONC	eConsent Trial	Improve patient education and engagement, so that patients can make an informed decision about how they would like to share their health information.	Use Limitation Patient consent
DHS	DHS S&T Privacy Working Group	DHS-wide Privacy Working Group convened to meet annually to gather requirements to address common capability gaps.	Protection of personally identifiable information (PII) collected for DHS mission purposes
DHS	Policy Reasoning Engine	Development of a policy reasoning engine to analyze privacy policies when information is shared across jurisdictions to ensure the policies and actions comply with applicable laws and regulations. Fostering confidence that personal information is being shared appropriately, thus minimizing privacy breaches.	Automating privacy compliance Policy-compliant sharing of privacy information
DHS	Future (unnamed) project	Securing access to PII in information sharing environments.	Privacy Policy Compliance Tools Privacy-Preserving Federated Search Mobile Computing Privacy (tools to protect location-privacy) Privacy-preserving methods for research and testing Anonymization in Robotic Aircraft for Public Safety Surveillance
NIST	Privacy Engineering Program	Support implementation of effective and measurable privacy mechanisms in IT systems. Focus on the current gap between privacy principles and repeatable and measurable ways to implement these principles.	Currently developing a plan to determine the initial direction and deliverables of the program

NIST	Executive Order 13636: Improving Critical Infrastructure Cybersecurity	Development of a framework to reduce cybersecurity risks to critical infrastructure, in a way which also protects individual privacy and civil liberties.	Advancement and application of Fair Information Practice Principles, in the Framework under the EO-13636
NIST	National Strategy for Trusted Identities in Cyberspace	Public-private collaboration to create an Identity Ecosystem – a marketplace of more secure, convenient, interoperable, and privacy-enhancing solutions for online authentication and identification.	Mitigating privacy and civil liberties risks arising from the potential for increased identification, tracking, and personal data aggregation in the Identity Ecosystem
NIST	Research on Privacy-enhancing Technologies (PETs)	PETs offer the capability to automate key privacy principles around data minimization, individual control of personal information and security.	Revocable biometrics Cryptographic-based PETs
NIST	Security and Privacy Controls for Federal Information Systems and Organizations, Special Publication (SP) 800-53, Revision 4	SP 800-53, Revision 4, Appendix J provides a structured set of privacy controls to help organizations comply with applicable federal laws.	Implementation of the Fair Information Practice Principles
NIST	Smart Grid	NIST is actively involved in the Smart Grid Interoperability Panel Privacy Subgroup to address the privacy impact that emerging smart grid technologies, policies, business models, and consumer transactions may have on consumers' personal data.	Standards development for the smart electronic power grid with support for privacy
NIST	Social Media and Message Formats	Develop security guidelines and best practices that incorporate the usability principles of efficiency, effectiveness, and user satisfaction.	Personal data sharing
NIST/NSTIC	Exponent	Develop secure, easy-to-use and privacy-enhancing credentials for users	Privacy-enhancing credentials

NIST/NSTIC	Georgia Tech Research Corporation (GTRC)	Develop and demonstrate a "Trustmark Framework" that seeks to improve trust, interoperability and privacy within an identity ecosystem.	Trust framework
NIST/NSTIC	Privacy Vaults Online, Inc.	Develop COPPA-compliant, secure, privacy-enhancing credentials with a service for use at Internet scale.	COPPA-compliant, secure, privacy-enhancing credentials
NIST/NSTIC	ID.me, Inc.	Develop and pilot trusted identity solutions that will allow military families to access sensitive information online from government agencies, financial institutions and health care organizations.	Privacy-enhancing, trusted identity solutions
NIST/NSTIC	Transglobal Secure Collaboration Participation, Inc.	Deploy trusted credentials to conduct secure business-to-business, government-to-business and retail transactions for small and medium-sized businesses.	Trusted credentials
NIST/NSTIC	American Association of Motor Vehicle Administrators	Pilot the Cross Sector Digital Identity Initiative (CSDII).	Identity management
NIST/NSTIC	Criterion Systems	The pilot will allow consumers to selectively share shopping and other preferences and information to both reduce fraud and enhance the user experience.	Privacy-enhancing online transactions
NIST/NSTIC	Daon, Inc.	Develop and user-friendly identity solutions that leverage smart mobile devices to maximize consumer choice and usability.	Trusted interactions with multiple parties online
NIST/NSTIC	Resilient Network Systems, Inc.	Develop a Trust Network built around privacy-enhancing encryption technology to provide secure, multifactor, on-demand identity proofing and authentication across multiple sectors	Trusted online access, sharing of online resources while protecting privacy and confidentiality

NIST/NSTIC	University Corporation for Advanced Internet Development (UCAID)	Develop a privacy infrastructure through common attributes, user privacy managers, anonymous credentials, and Internet2's InCommon Identity Federation service	Multifactor authentication Identity management
NIH/NCI	Statistical methods for risk of disclosing the identities of cancer patients in a cancer registry database	Develop novel statistical methods to evaluate the probability of disclosing the identities of cancer patients.	Incremental risk of disclosure of patient information when certain geography details are released in addition to patients' demographics
NIH/NCI	Research on releasing census tracts in cancer registry data while maintaining confidentiality	Develop approaches for generating simulated tract identifiers to release with cancer registry microdata files.	Evaluating trade-off between privacy protection and statistical data integrity
NIH/NIGMS	iDASH: Integrating Data for Analysis, Anonymization, and Sharing	Develop new algorithms, tools, computational infrastructure and services that will enable biomedical and behavioral researchers to integrate Data for Analysis, Anonymization, and Sharing, in a secure, privacy-preserving environment.	Privacy protection through anonymization, data simulation, and an informed consent management system Secure and confidential access to human subject data for research
NIH/NIGMS	TRIAD: Tools and Resources for Inappropriate Access Detection in EHRs	Advance research on preventing inappropriate access to electronic health records (EHR) by insiders. Make research data available for privacy technology research without compromising patient, user, or institutional privacy.	Real-time algorithms for inappropriate access prevention to EHR
NIH/NLM	Extramural grants	From 2000 to 2013 NLM has expended approx. $40M to fund 35 grants in privacy-protection topics of biomedical informatics.	Privacy of personal health information Computational techniques related to privacy, data access and data sharing
NIH/NLM	Scalable and Robust Clinical Text De-Identification Tools	Current de-identification approaches severely limit the use of clinical text while exposing patients to privacy risks. We developed an alternative approach, the	Privacy preserving de-identification of clinical information

		strategy of concealing. We call it "Hiding In Plain Sight" (HIPS) which replaces all known PHI with "surrogate" PHI- fictional names, ages, etc.-that look real but do not refer to any actual patient.	
NIH/NLM	New Technology to Preserve Patient Privacy and Data Quality in Health Research	Develop a novel data-masking technology that can be used by healthcare organizations to prevent or limit privacy disclosure when sharing patient data for research.	Privacy of personal health information in research
NIH/NLM	Technologies to Enable Privacy in Biomedical Databanks	Develop a novel data protection model for centralized person-specific biomedical records.	Privacy of personal health information in research
NIH/NLM	Secure Sharing of Clinical History & Genetic Data: Empowering Predictive Personalized Medicine	Develop and evaluate privacy-preserving data mining algorithms for use with original (not anonymized) data sets. Develop and evaluate anonymizing data publishing algorithms and privacy guarantees.	Privacy of personal health information in research
NSF	Secure and Trustworthy Cyberspace (SaTC) program	Approximately 35% of the FY13 SaTC program (110 new research grants ranging from $100K/2 years to $10M/5 years, for the total of $65M) is in whole or large part related to privacy.	A broad range of privacy topics.
NSA	New Mechanisms for Trustworthy Platforms	Design of computing mechanisms to provide confidentiality, integrity, and authentication of software.	New computing paradigms that protect user data privacy and organizational equities in third-party computing platforms.
NSA	Basic and Applied Cryptographic Research	Design of cryptographic primitives to provide basic security services of confidentiality, integrity, and authentication.	Cryptographic primitives that support privacy applications Protocols for anonymous signatures, key establishment, and group keying schemes
NSA	Private Information Retrieval (PIR)	Research and study of PIR techniques for use in government applications.	Querying of data without disclosing what the query is seeking

NSA	Homomorphic Encryption	Advance techniques that allow one to conduct operations on encrypted data that provide an encrypted result.	Processing of private data, in encrypted form, without knowledge of the data
IARPA	Security and Privacy Assurance Research (SPAR) Program	Research to improve the ability to share information while protecting the security and privacy interests of each party by protecting both the confidentiality of a query and preventing disclosure of any record other than those that match the query.	Privacy-preserving database access protocols Applications of homomorphic encryption techniques to data retrieval Secure publish-subscribe protocols
ONR	Traffic-secure Routing Using System Trust	Develop a theory of trust-based traffic security: creating and investigating the models to understand traffic-secure routing in diversely trusted networks.	Anonymity: design & analysis of private communication over systems and networks that are under adversary control
ONR	Protocols and Policies in Security and Networking	Privacy-aware policy for communicating private information.	Collaborative planning with confidentiality
ONR	Networks Opposing Botnets (NoBot)	Develop techniques and tools for in-network defense using cooperating programmable elements for correlating, detecting, adapting to and neutralizing large scale malicious behaviors in the network.	Differential privacy query language to provide strong privacy guarantee in collaborative environment
ONR	Leveraging Formal Techniques to Harden Mobile Platforms	Improve the security of mobile platforms by providing new protection mechanisms that make it feasible to conveniently specify rich security policies.	Protection of personal information stored in personal mobile devices

Summary

Current activities contributing to privacy research suggest that they can be broadly grouped into four areas:

Research areas	**Support for privacy as an extension of security**	**Privacy characterization and compliance**	**Privacy in healthcare**	**Privacy research explorations**
Agencies	AFRL, DARPA, NSA, IARPA, ONR	DOE, DHS, NIST	TATRC, ONC, NIH	NSF
Funding estimate ($77M/year)	$34M/year	$10M/year	$8M/year	$25M/year
Key topics	Access restriction Anonymity Security policy integration Privacy preserving data aggregation Privacy in third-party computation Cryptographic primitives for privacy Private information retrieval Homomorphic encryption Privacy-preserving database access protocols Traffic-secure routing Confidential collaboration and communication Security policies for mobile devices	Voluntary code of conduct for SmartGrid Protection of PII Automated privacy compliance Privacy-preserving methods for research Location-privacy tools Critical infrastructure cybersecurity risk framework Identity ecosystem marketplace Standards for legal compliance	Patient privacy Patient consent Patient privacy policies Patient data quality Security and privacy tools and methods for electronic health information Data segmentation for privacy Use limitation Collection limitation Preserving anonymity in healthcare statistical and research data Anonymization Access control to patient data	Formulation of privacy in terms of access to information Formulation of privacy as a social-psychological construct Privacy policy formulation, specification, enforcement, analysis Algorithmic foundations for privacy and tools Economics of privacy, privacy metrics Usability aspects of privacy Privacy – Security - Usability trade-offs Privacy preserving solutions for data integration, mining, querying Privacy preserving solutions for cloud computing

Comments and Next Steps

PCAST's 2010 and 2013 reports on NITRD call on federal agencies to create a multi-agency research initiative to develop scientific and engineering foundations for privacy for the digital era. Such foundations should serve as the basis for a range of technologies and solutions to enable us reconcile individual privacy protection with the benefits of large-scale networking and IT systems and services. The NITRD survey of privacy research indicates that agencies are funding research in many areas related to privacy, including scientific foundations.

The following questions are offered for further discussions in assessing and developing NITRD privacy research agenda:

- Context:
    - What are the key concerns about privacy in cyberspace?
    - What techniques, methods, or capabilities, if we had them today, would alleviate concerns about privacy in cyberspace?
    - How do social science and law view technical privacy issues?
    - What guidance can the Fair Information Practice Principles (FIPPs) and the "Consumer Privacy Bill of Rights[4]" provide for research in privacy?
- Research motivations and requirements:
    - What is the relationship between privacy and security? Are there any mutually exclusive properties of privacy and security?
    - Privacy is contextual and dependent on one's expectation of what happens with disclosed information. How can science and engineering address the context and expectations?
    - What unique research requirements are presented by government?
    - What research requirements come from the private sector?
- Research goals:
    - Is there privacy research that is different from research in security? If yes, what would be the unique research objectives and activities?
    - What are the major challenges to be solved: in computer science, in law, in sociology and psychology, other fields?
- Methods:
    - What options exist (or need to put in place) within the Federal government for multi-agency coordination and collaboration in privacy research?
    - How should various disciplines work together?
    - How should the research community interact with civil society and consumer advocacy organizations?

[4] "Consumer Data Privacy in a Networked World: a Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," The White House, February 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf