

## **Request for Information (RFI) – National Privacy Research Strategy**

AGENCY: The National Coordination Office (NCO) for Networking and Information Technology Research and Development (NITRD).

ACTION: Request for Information (RFI)

FOR FURTHER INFORMATION, CONTACT: Tomas Vagoun at [vagoun@nitrd.gov](mailto:vagoun@nitrd.gov) or (703) 292-4873.

DATES: To be considered, submissions must be received no later than October 17, 2014.

### **SUMMARY:**

Agencies of the Federal Networking and Information Technology Research and Development (NITRD) Program are planning to develop a joint National Privacy Research Strategy. On behalf of the agencies, the Cyber Security and Information Assurance Research and Development Senior Steering Group seeks public input on the vital privacy objectives that should be considered for the goals of the strategy. The National Privacy Research Strategy will be used to guide federally-funded privacy research and provide a framework for coordinating research and development in privacy-enhancing technologies.

### **SUPPLEMENTARY INFORMATION:**

#### Background:

Life in the 21<sup>st</sup> century is inextricably interconnected with cyberspace and information systems. The computing revolution is enabling advances in many sectors of the economy, but at the same time our social realm has been profoundly affected by the rise of the Internet. Privacy in the digital era is challenged by our capabilities to store and process vast quantities of information. On the one hand, large-scale data analytics is indispensable to progress in science and engineering, but on the other hand, when information about us and our activities in cyberspace can be tracked and repurposed without our understanding, opportunities for crime, discrimination, and misuse are created.

Respect for privacy is a cornerstone principle of our democracy. A variety of laws and policies guide collection and use of data by the government, corporations, and organizations. However, because technology advances can outpace law, respect for privacy must be a guiding principle in the technological domain and our information systems must be designed to provide the means for protecting privacy.

Privacy harms to individuals can arise from actions taken with personal information, including from unapproved disclosure of personal information, to tracking and profiling of our actions, preferences, and habits in cyberspace, to analytical inferences from unrelated data sources. Protection of privacy in this context will require the development of both specific technologies targeted for particular use, as well as foundational science and engineering to develop the capabilities to be able to analyze the situations in the digital realm that might lead to privacy harms, and respond with actions and technologies to prevent or mitigate them.

The Federal Government already plays an important role in protecting certain aspects of privacy, as directed by various legislation (e.g., HIPAA, COPPA), and this Administration has further championed a number of initiatives (such as the “Consumer Privacy Bill of Rights” proposal) to improve the state of privacy. In the technical domain, Federal agencies already fund research aimed at a wide range of privacy aspects, from basic research to specific technologies (see [1] for a summary of Federal research in privacy). Nevertheless, privacy in the digital age is a topic of national (and global) importance and more needs to be done. Many challenges remain in areas such as privacy-preserving solutions for data integration and data mining, methods and solutions for managing privacy in electronic health information systems, usage-based controls on privacy and techniques to express user preferences related to data use, or methods for quantifying risks and harms to privacy of individuals. Furthermore, new technologies such as wearable computing (e.g., glasses with cameras, biomedical sensors), embedded computing (e.g., Internet of Things), or cyber-physical systems (e.g., the Smart Grid) create new contexts in which privacy can be challenged and that require targeted technologies to support personal privacy.

#### Objectives:

Reports by the White House and the President’s Council of Advisors on Science and Technology (PCAST) on big data and privacy [2] and [3], and reports on Federal networking and information technology research [4] and [5], call for serious increases in investments for research and development (R&D) in privacy-enhancing technologies and in encouraging multi-disciplinary research involving computer science, social science, and legal disciplines. The White House and PCAST cite challenges to personal privacy in the digital era as a significant impairment that is undermining societal benefits from large-scale deployments of networking and IT systems.

At the request of the White House Office of Science and Technology Policy (OSTP), the Cyber Security and Information Assurance Research and Development Senior Steering Group (CSIA R&D SSG) of the Federal Networking and Information Technology Research and Development (NITRD) Program [6] will lead the development of a National Privacy Research Strategy (NPRS). The NPRS will establish objectives and prioritization guidance for federally-funded privacy research, provide a framework for coordinating R&D in privacy-enhancing technologies, and encourage multi-disciplinary research that recognizes the responsibilities of the Government, the needs of society, and enhances opportunities for innovation in the digital realm. The NPRS will be a catalyst to concentrate Federal research resources against critical privacy challenges and to provide enduring objectives for research in privacy-enhancing technologies. The strategy will be developed by interagency collaboration and in a partnership with commercial and academic sector stakeholders and citizens interested in addressing the privacy needs of the nation.

The CSIA R&D SSG is issuing this Request for Information (RFI) to solicit input from the public on defining the most important goals for privacy in the digital world. As a strategy, the NPRS must focus research activities toward relevant and impactful objectives, and this RFI seeks to inform our understanding of societal needs where privacy-enhancing technologies would be beneficial. While there are social and legal solutions to many digital privacy issues, they are out of scope for the NPRS; our focus will be on the research directions for privacy-enhancing technologies, designs, and methods to enable privacy-

preserving information systems. The submissions received under this RFI will be used as inputs in structuring the strategy.

Request:

Through the NPRS, the CSIA R&D SSG seeks to establish objectives for research and a framework for organizing ideas to achieve the research purpose. Responders are asked to answer one or more of the following questions:

1. Privacy objectives: describe one or more scenarios that illustrate a critical issue concerning privacy; describe what privacy problems arise in the scenario; describe why it is important to overcome the identified problems; describe the needed privacy and what capabilities are required to achieve it; and describe what barriers exist to achieving the needed privacy in the scenario. The use of particular domains in the scenario (e.g., healthcare, education, social media) to describe the desired privacy state is encouraged.
2. Assessment capabilities: discuss concepts, methods, and constructs needed to assess privacy; discuss capabilities and models that can: express privacy requirements, assess and quantify risks/benefits to privacy, evaluate effects of privacy risk mitigation, and determine the fulfillment of privacy requirements.
3. Multi-disciplinary approach: discuss how privacy challenges and objectives might be framed to bring many disciplines (e.g., computer science, economics, social and behavioral sciences, and law disciplines) together to jointly and collaboratively work to both strengthen privacy and support innovation in cyberspace and information systems; discuss how diverse national/cultural perspectives on privacy can be accommodated.
4. Privacy architectures: (a) the Big Data report [2] recommends adoption of a "responsible use framework" [pg. 61] that would provide greater focus on the use of data and hold entities that utilize data accountable for responsible use of the data. Describe an architecture implementing a "responsible use framework" incorporating the three questions above and taking into account issues as: encoding privacy policies in machine-checkable forms and ensuring their compliance and auditability; managing the collection, retention, and dissemination of sensitive data; and ensuring the confidentiality and integrity of sensitive data, while enabling desired uses of them. (b) Describe other privacy architectures that would be effective for the design and implementation of privacy-preserving information systems. (c) Describe technological advances that can change privacy perceptions and how those advances would be incorporated into the "responsible use framework" architecture or other architectures submitted for 4(b).

Submission Instructions:

Page limitation: all submissions must be 20 pages or less.

Comments can be submitted by any of the following methods:

(a) Email: [nprs@nitrd.gov](mailto:nprs@nitrd.gov)

(b) Fax: (703) 292-9097, Attn: National Privacy Research Strategy

(c) Mail: Attn: National Privacy Research Strategy, NCO, Suite II-405, 4201 Wilson Blvd., Arlington, VA 22230

Deadline for Submission under this RFI is October 17, 2014.

Responses to this RFI may be posted without change online, at <http://www.nitrd.gov>. The CSIA R&D SSG therefore requests that no business proprietary information, copyrighted information, or personally identifiable information be submitted in response to this RFI.

In accordance with FAR 15.202(3), responses to this notice are not offers and cannot be accepted by the Government to form a binding contract. Responders are solely responsible for all expenses associated with responding to this RFI.

References:

[1] "Report on Privacy Research within NITRD," April 2014,  
[http://www.nitrd.gov/Pubs/Report\\_on\\_Privacy\\_Research\\_within\\_NITRD.pdf](http://www.nitrd.gov/Pubs/Report_on_Privacy_Research_within_NITRD.pdf)

[2] "Big Data: Seizing Opportunities, Preserving Values," May 2014,  
[http://www.whitehouse.gov/sites/default/files/docs/big\\_data\\_privacy\\_report\\_may\\_1\\_2014.pdf](http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf)

[3] "Big Data and Privacy: A Technological Perspective," May 2014,  
[http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast\\_big\\_data\\_and\\_privacy\\_-\\_may\\_2014.pdf](http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf)

[4] "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>

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

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