NATIONAL PRIVACY RESEARCH STRATEGY

A Report by the

PRIVACY RESEARCH AND DEVELOPMENT
INTERAGENCY WORKING GROUP

SUBCOMMITTEE ON NETWORKING AND INFORMATION
TECHNOLOGY RESEARCH AND DEVELOPMENT

of the

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

JANUARY 2025

Table of Contents

1. Executive Summary

People's lives are inextricably interconnected with cyberspace and information systems. The computing revolution has enabled advances in many sectors of the economy, while social interactions have been profoundly affected by the rise of the Internet, mobile communications, and rapid advances in artificial intelligence (AI), including recent fast-paced growth of large language models (LLMs) or foundational models trained on large amounts of data. Ever-increasing computational power, hyperconnectivity online, and exponential growth of powerful data collection devices and techniques in a wide range of application domains, such as transportation, education, health care, and finance, are accelerating these trends. Massive data collection, storage, processing, and retention in the digital era challenge long-established privacy norms and introduce significant risks of privacy harms to individuals with negative consequences to communities and society at large. The increased ability to conduct data analytics at scale, including training large and powerful AI models, is indispensable to progress in science, engineering, medicine, and social good. However, when information about individuals and their activities can be tracked, combined, inferred, and repurposed without their knowledge or understanding, risks emerge that these data actions could result in such individuals experiencing physical harm, unfair discrimination, loss of autonomy, financial loss, and loss of dignity. The presence of these privacy risks can have a devastating and chilling effect on people's behaviors, diminish public trust in cyberspace, and exacerbate potential harm to both individuals and society.

The federal government is mindful of these privacy risks and the critical need for foundational, use-inspired and translational privacy research and development (R&D). The Executive Order on Safe, Secure and Trustworthy Development of AI (EO 14110)[1] emphasizes that "Americans' privacy and civil liberties must be protected as AI continues advancing," and that the agencies "shall use available policy and technical tools, including privacy-enhancing technologies (PETs) where appropriate to protect privacy." The Executive Order on Ensuring Responsible Development of Digital Assets (EO 14067) highlights the need for protecting consumer and other stakeholders by ensuring privacy protection and safeguards against "unlawful surveillance."[2] Similarly, the Blueprint for an AI Bill of Rights[3] emphasizes the need for data privacy reinforcing the message to individuals: "you should be protected from abusive data practices via built in protection and you should have agency over how data about you is used."

This National Privacy Research Strategy (NPRS) updates the 2016 NPRS and outlines the strategic priorities for privacy R&D to be pursued by researchers and practitioners from public and private sectors. It establishes objectives for federally funded (both extramural and government-internal research) as well as industry-funded privacy R&D, provides a common direction for coordinating R&D in privacy-preserving technologies, and encourages multidisciplinary research that recognizes the responsibilities of public-private stakeholders and the needs of society at large.

---

[1] The White House. (2023, October). *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

[2] The White House. (2022, March). *Executive Order on Ensuring Responsible Development of Digital Assets.* https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/

[3] The White House Office of Science and Technology Policy (OSTP). (2023). *Blueprint for an AI Bill of Rights*. https://www.whitehouse.gov/ostp/ai-bill-of-rights/

The overarching goal of this strategy is to promote innovative privacy research and privacy-preserving technology while advancing the well-being and prosperity of individuals and society.

To achieve these goals, this strategy identifies the following priorities for privacy research:

- Foster multidisciplinary approaches to privacy research and solutions;
- Understand and measure privacy preferences and impacts;
- Develop system design methods that incorporate privacy preferences, requirements, and controls;
- Increase transparency of data collection, sharing, use, and retention;
- Ensure that information flows and use are consistent with privacy rules; and
- Reduce privacy risks of data analytics and AI, including the potential of re-identifying anonymized data.

2. Introduction

2.1 Privacy Research Purpose

Networking and information technology is transforming life in the 21st century, changing the way people, businesses, and government interact at scale. Vast improvements in computing, storage, and communications technologies, including rapid progress in AI and advanced analytics, are creating unprecedented opportunities for enhancing individuals' social wellbeing; improving health and health care; eliminating barriers to education and employment; and increasing efficiencies in many sectors, such as manufacturing, transportation, finance, and agriculture.

Advances in information technology have mixed results. For example, the promise of these new systems and applications often stems from their ability to create, collect, store, transmit, process, and archive information on a massive scale. However, the exponential growth in the quantity of personal information that is being collected and retained, combined with the increased ability to analyze it and combine it with other information, is creating valid concerns about privacy risks and about the ability to manage these unprecedented volumes of data responsibly. The presence of such risks can create a chilling effect on people's behaviors and rapidly reduce trust in cyberspace.

However, the progress of privacy understanding, and experience under legal and regulatory protections, has not kept pace with the exponential increase in data collection, processing, and storage, and the resulting risks to privacy. Today, information exists in a complex and dynamic ecosystem that includes:

- Individuals whose information and data elements are collected, processed, or stored;
- Data collectors and data brokers, who buy, repackage, and sell collected information;
- Analytics providers, including AI model developers, who create systems for processing such information to extract valuable insights from data;
- Data managers, who maintain data that may include sensitive records or when combined with other data could risk privacy harms; and
- Data users, who make decisions based on the data analytics.

The decreasing cost of storage has enabled organizations to collect large amounts of data and save the data in long-term repositories, making such data available for unanticipated or even unforeseeable future use. Meanwhile, there is a growing array of ubiquitous consumer devices, environmental sensors, and tracking technologies designed to collect, process, and archive information continuously, often