

Testimony of

Dr. Charles H. Romine
Director
Information Technology Laboratory

National Institute of Standards and Technology
United States Department of Commerce

Before the
United States House of Representatives
House Committee on Science, Space and Technology
Subcommittee on Investigations and Oversight

“Privacy in the Age of Biometrics”

June 29, 2022

Chairman Foster, Ranking Member Obernolte, and distinguished members of the Subcommittee, I am Charles Romine, the Director of the Information Technology Laboratory (ITL) at the Department of Commerce's National Institute of Standards and Technology – known as NIST. Thank you for the opportunity to testify today on behalf of NIST on our efforts to evaluate the privacy implications of biometrics technologies.

NIST is home to five Nobel Prize winners, with programs focused on national priorities such as artificial intelligence, advanced manufacturing, the digital economy, precision metrology, quantum information science, biosciences and, of course, cybersecurity. The mission of NIST is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

In the NIST Information Technology Laboratory, we work to cultivate trust in information technology and metrology. Trust in the digital economy is built upon key principles like cybersecurity, privacy, interoperability, equity, and avoiding bias in the development and deployment of technology. NIST conducts fundamental and applied research, advances standards to understand and measure technology, and develops tools to evaluate such measurements. Technology standards—and the foundational research that enables their development and use—are critical to advancing trust in and promoting interoperability between digital products and services. Critically, they can provide increased assurance, thus enabling more secure, private, and rights-preserving technologies.

NIST Privacy Engineering Program

Since its establishment nearly a decade ago, NIST's Privacy Engineering Program's mission has been to support the development of trustworthy information systems by applying measurement science and system engineering principles to the creation of frameworks, risk models, guidance, tools, and standards that protect privacy and, by extension, civil liberties.

The program has worked to fill gaps in the field of privacy and advance the foundations of privacy risk management by introducing a generalizable model for identifying privacy risks in systems processing data and a set of privacy engineering objectives in its seminal publication NISTIR 8062, [An Introduction to Privacy Engineering and Risk Management in Federal Systems](#).

The program has produced a number of tools to assist organizations in managing privacy risk. For example, the NIST Privacy Risk Assessment Methodology provides organizations with the capability to identify and prioritize privacy risks in the systems, products, and services that they are designing or deploying. The ability to conduct thorough privacy risk assessments is essential for organizations to select effective mitigation measures, including appropriate privacy-enhancing technologies.

NIST Privacy Framework

Modeled after NIST's highly successful Cybersecurity Framework, the NIST Privacy Framework is another voluntary tool developed in collaboration with stakeholders through a

public and transparent process. It is intended to support organizations' decision-making in product and service design or deployment to optimize beneficial uses of data while minimizing adverse consequences for individuals' privacy and society as a whole.

Designed to complement existing business and system development operations, the framework can help organizations answer the fundamental question, "*How are we considering the privacy risks to individuals as we develop or deploy our systems, products, and services?*" To account for an organization's unique needs, the framework provides flexibility in implementation and is law- and technology-agnostic so that it can be used by organizations of all types around the world. Rather than prescribing requirements, the framework provides the building blocks for organizations to consider the policies and the technical capabilities needed to achieve their privacy objectives.

The Privacy Framework leverages the Privacy Engineering Program's privacy risk model by promoting the analysis of privacy events as potential problems individuals could experience arising from system, product, or service operations with data, whether in digital or non-digital form, through a complete life cycle from data collection through disposal. These data operations are described in the singular as a data action and collectively as data processing. The problems individuals - whether singly, in groups, or at the societal level - can experience as a result of data processing can be expressed in various ways, but NIST describes them as ranging from dignity-type effects such as embarrassment or stigmatization to more tangible harms such as discrimination, economic loss, or physical harm. When these externalities are made more visible to organizations, they are in a better position to bring privacy risk into parity with other risks in their enterprise risk management portfolio and drive more informed decision-making about resource allocation to strengthen privacy programs.

Structurally, the core of the framework provides an increasingly granular set of activities and outcomes that enable organizational dialogue and prioritization around managing privacy risk. It is organized around five Functions: Identify, Govern, Control, Communicate, and Protect. The Functions are further divided into Categories and Subcategories. As previously mentioned, the framework is technology-agnostic. Although biometrics are not specifically referenced, the framework can be applied to biometrics systems equally as well as any other technology. For example, the Disassociated Processing Category is focused on NIST's disassociability privacy engineering objective, which promotes the design of system capabilities for processing data or events without association to individuals or devices beyond the operational requirements of the system. This disassociation can be realized through different methods expressed in the various Subcategories.

One of the Subcategories describes the outcome that data are processed to limit observability and linkability by, for example, having data actions take place on local devices or using privacy-enhancing cryptography. Biometrics are often used to link an action with someone's identity. Matching a biometric stored on a local device with the user can lower the privacy risk in comparison with matching against a centrally stored database of biometrics, where there is a higher risk of a data breach or scope creep – or in other words, the biometrics could be used in ways that exceed individuals' or society's expectations or desires based on the initial collection. Nonetheless, there may be use cases where a centralized database is necessary.

The Privacy Framework conception of privacy is not binary in that it does not take the view that privacy either exists or does not exist, but instead conceives of privacy as existing alongside other needs in different contexts. The purpose of privacy risk management is to identify how privacy risks may change in these different contexts and determine appropriate mitigation measures with the understanding that it is no more possible to eliminate all privacy risk than it is to eliminate all security risk. Thus, organizations that might need to employ centralized databases could use other mitigation techniques such as privacy-enhancing cryptography. There are various types of privacy-enhancing cryptography that can be used for different purposes. For instance, some types of cryptography permit computational processing on data while they remain in an encrypted state. This application could provide greater privacy protections for biometric databases by enabling data analytics while eliminating the need to expose the raw data to other entities. Ultimately, risk management can help to effectively address and manage privacy risk and adverse impacts, leading to more trustworthy biometric systems or non-biometric alternative measures as appropriate.

A second Subcategory articulates that data are processed to limit the identification of individuals. Differential privacy is another type of privacy-enhancing technology, which can be used to generate datasets for statistical analysis without revealing whether any particular individual's information is contained in the dataset. NIST maintains more than a dozen open-source differential privacy tools as well as the winning algorithms from its series of differential privacy prize challenges in its Privacy Engineering Collaboration Space - a virtual, public platform for sharing tools and use cases to advance privacy-enhancing technologies. Having recently completed a blog series on how to implement differential privacy, NIST is preparing to release a first draft of more in-depth guidelines. Although using differential privacy for image data is an area that requires further research, conceivably it could provide significant benefits for the privacy of individuals in areas such as healthcare research by enabling analysis of biometric images in health records without being able to link them to specific individuals.

A third Subcategory describes the outcome that data are processed to limit the formulation of inferences about individuals' behavior or activities such as through decentralized data processing or distributed architectures. Techniques such as federated learning enable the training of models across distributed datasets in lieu of more traditional methods requiring centralizing datasets in one location. Combined with some of the above-described privacy-enhancing technologies, federated learning could allow model training on biometric databases without having to risk combining datasets and increase the potential to learn more about individuals' behavior or activities.

NIST Privacy-Enhancing Cryptography

NIST has fostered the development of cryptographic techniques and technology for 50 years through an open process which brings together industry, government, and academia to develop workable approaches to cryptographic protection that enable practical security. Our work in cryptography has continually evolved to meet the needs of the changing IT landscape. As part of NIST's statutory responsibility under the Federal Information Security Modernization Act (FISMA), NIST researchers develop cryptographic standards and guidelines that are used throughout the world to protect information at rest and in transit. Through Federal Information

Processing Standards (FIPS) and NIST Special Publications, and participation in national and international standards developing organizations (SDOs), NIST specifies foundational cryptographic algorithms and mechanisms for encryption, message authentication, and digital signatures to protect the confidentiality and integrity of data. The NIST algorithms and associated cryptographic guidelines are developed in a transparent and inclusive process, leveraging cryptographic expertise around the world. The results are strong, interoperable, and broadly-supported cryptographic mechanisms that can be used by all industries in a variety of applications and use cases.

To support current and future cybersecurity needs, NIST maintains a broad cryptographic research program that studies and advances emerging technologies and techniques in cryptography. Through active engagement with our federal and industry partners that use our standards and guidelines, along with collaboration with academic researchers, NIST works to better understand how cryptographic tools can address critical challenges facing our nation. The results of this research program help to drive the development of new standards and guidelines, such as in the area of quantum-resistant cryptography. One focus area for our cryptographic research program is privacy-enhancing cryptography— studying how advanced cryptographic techniques, such as multiparty computation, zero knowledge proofs, and homomorphic encryption, can allow systems to share or process data in a privacy preserving manner. Working with our industry and academic partners, we are working to research the security of these new techniques and to develop reference materials to facilitate their adoption in standards, applications, and systems. As with other cryptographic mechanisms, these techniques have the potential to be broadly applied to different use cases— from protecting biometric data and comparison algorithms, to facilitating new models of information sharing between organizations without revealing sensitive information.

Biometric Data Storage and Processing Standards

Since the 1980s NIST has coordinated development of the ANSI/NIST-ITL Standard “Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information,” for interchange of biometric data in law enforcement applications, extending the modalities from fingerprint to include face, iris, voice and DNA. The standard establishes procedures for collecting and processing of the data needed to instantiate the records, particularly regarding quality assessment, and the application of compression. The standard is used globally by law enforcement, homeland security, defense, intelligence agencies, and other identity management systems and owners/developers to ensure biometric information interchanges are interoperable, and maintain system integrity and efficiency. While the last major update to ANSI/NIST-ITL was in 2015, the standard is currently under review and the next major update is in progress.

Since 2002, NIST has also supported development of international standards (in ISO/IEC) for data interchange in, primarily, civil applications including ID cards including e-passports.

Different uses of biometrics – for example, as authenticators to protect access to sensitive data, or convenient entry solutions and fraud prevention -- give rise to different degrees of privacy risk. Organizations need to have the means to be able to distinguish between the different degrees of privacy risk and implement appropriate mitigation measures. The NIST Privacy Framework provides the structure for organizations to consider which privacy-protective

outcomes are suitable to their use cases. The NIST Privacy Risk Assessment Methodology helps them to identify the specific privacy risks arising from their systems in order to determine appropriate mitigations. The research on privacy-enhancing technologies that NIST conducts and the guidelines and standards that NIST publishes helps organizations in implementing effective mitigations appropriately tailored to identified risks.

Privacy-Enhancing Technologies Research

Privacy plays a critical role in safeguarding fundamental values such as human autonomy and dignity, as well as civil rights and civil liberties. NIST has prioritized measurement science research and the creation of frameworks, guidance, tools, and standards that protect privacy. In addition to maintaining the NIST Privacy Framework, NIST also includes privacy considerations in many of NIST's critical cybersecurity guidelines, as well as the draft AI Risk Management Framework.

NIST is also collaborating with the Office of Science and Technology Policy and the National Science Foundation to advance privacy-preserving data sharing and analytics through bilateral prize challenges with the United Kingdom's Department for Digital, Culture, Media and Sport. The prize challenges were a U.S. deliverable in the Summit for Democracy's Presidential Initiative for Democratic Renewal and are expected to launch this summer with winning solutions to be showcased at the second Summit for Democracy.

Conclusion

Advancing cybersecurity, privacy, and biometrics research and standards that ensure a secure, private, and interoperable digital economy is a significant priority for NIST. Our economy is increasingly global, complex, and interconnected. It is characterized by rapid advances in technology. The timely availability of international cybersecurity, privacy and biometrics standards and guidance is a dynamic and critical component to ensure the resilience of such advances in technology. With robust collaboration with stakeholders across government, industry, international bodies, and academia, NIST aims to cultivate trust and foster an environment that enables innovation on a global scale.

Continuing research on privacy-enhancing technologies through various mechanisms such as prize challenges, pilot collaborations, and guidance publications to increase their maturity and promote their widespread adoption is a priority for NIST.

My staff at NIST are some of the top cybersecurity, privacy, biometrics, artificial intelligence and standards experts in the world. Working with our partners in other federal agencies, the private sector, academia, and other countries, and with the support of Congress, we will work tirelessly to address current and future emerging technology challenges.

Thank you for the opportunity to present on NIST activities on privacy enhancing technologies for biometric applications. I look forward to your questions.



Charles H Romine (Fed)

Director, Information Technology Laboratory

Charles Romine is Director of the Information Technology Laboratory (ITL). ITL is one of six research Laboratories within the National Institute of Standards and Technology (NIST) with an annual budget of \$120 million, nearly 400 employees, and about 200 guest researchers from industry, universities, and foreign laboratories.

Romine oversees a research program that cultivates trust in information technology and metrology by developing and disseminating standards, measurements, and testing for interoperability, security, usability, and reliability of information systems. ITL develops and disseminates cybersecurity standards and guidelines for Federal agencies and U.S. industry. ITL supports these and measurement science at NIST through fundamental and applied research in computer science, mathematics, and statistics. Through its efforts, ITL supports NIST's mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Within NIST's traditional role as the overseer of the National Measurement System, ITL is conducting research addressing measurement challenges in information technology as well as issues of information and software quality, integrity, and usability. ITL is also charged with leading the nation in using existing and emerging IT to help meet national priorities, including developing cybersecurity standards, guidelines, and associated methods and techniques, cloud computing, electronic voting, smart grid, homeland security applications, and health information technology.