Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.
BY ELECTRONIC MAIL

Mr. Suresh Venkatasubramanian
Assistant Director, Science and Justice
Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, D.C. 20504

Re: Document No. 2021-21975: NEC Corporation of America Comments in Response to the Office of Science and Technology Policy’s Request for Information on Public-Sector and Private-Sector Uses of Biometric Technologies

Mr. Venkatasubramanian:

NEC Corporation of America (NEC) is pleased to submit comments in response to the Office of Science and Technology Policy (OSTP) Request for Information (RFI) regarding public and private sector uses of biometric technologies.1 As a key member of the information and communications technology (ICT) industry and a major global supplier of biometric technologies, NEC appreciates OSTP’s effort to learn about biometric technologies from a variety of stakeholders while working to develop an AI Bill of Rights. We are committed to building digital trust by producing biometric technologies that are reliable, secure, and supportive of human rights and social justice, and we support OSTP’s efforts to seek information about biometric technologies and input on approaches to governing the use of biometric technologies.

We respectfully submit these comments to share information pertaining to several topics in the RFI, including: (1) descriptions of use of biometric information for recognition and inference; (2) procedures for and results of data-driven and scientific validation of biometric technologies; (3) security considerations associated with a particular biometric technology; (4) exhibited and potential harms of a particular biometric technology; (5) exhibited and potential benefits of a particular biometric technology; and (6) governance programs, practices, or procedures applicable to the context, scope, and data use of a specific use case.

I. Overview of NEC and Our Biometric Technologies

NEC delivers one of the industry’s strongest and most innovative portfolios of biometrics, security, analytics, and ICT solutions for enhanced customer experience, safety, and productivity. Headquartered in Irving, Texas, NEC (https://www.necam.com/) is a subsidiary of NEC Corporation, a global technology firm with $28 billion in annual revenue, a presence in over 160 countries and regions, and more than 110,000 employees worldwide. NEC Corporation has had a presence in the United States since 1963, and, today, our major U.S. offices span 16 states and employ over 2,000 people. One of the world’s top patent-producing companies, NEC Corporation combines advanced technologies, services, knowledge, and our 120 years of operating experience to help promote safety, security, fairness, and efficiency and build a more sustainable world in which all people have the opportunity to reach their full potential.

For over thirty years, NEC has been a leader in the biometrics industry. We invest significant resources in research and development and proudly provide both public-sector and private-sector customers with effective, efficient, and secure biometrics solutions, including predictive genotyping technologies and unimodal and multimodal face, voice, iris, fingerprint, latent print, palm print, and tenprint technologies.

---

2 We have also developed ear acoustic and gait recognition capabilities.
We began our biometrics business as a leading provider of Automated Fingerprint Identification Systems (AFIS) to state and local law enforcement agencies, and we built on our law enforcement expertise to become a trusted biometric technology provider to the U.S. Federal Government. Additionally, we provide commercial customers in the aviation, health care, entertainment, financial services, and hospitality industries with a variety of unimodal and multimodal biometric solutions.

U.S. Customs and Border Protection (CBP) uses NEC’s face recognition algorithm to fulfill its Biometric Entry/Exit mandate and improve security and traveler experiences at air, land, and maritime ports of entry in the United States. CBP has built and implemented its biometrics capabilities through public-private partnerships with airlines and airports that are working to modernize air travel and keep pace with the customer experience and security demands in the global aviation market. CBP’s biometrics programs have been the subject of numerous audits and reviews, including Privacy Impact Assessments, Government Accountability Office (GAO) reports, and congressional hearings. These reviews and audits have highlighted the accuracy of NEC’s algorithm, the numerous data privacy and cybersecurity protections that CBP and its partners leverage to safeguard traveler data, and the overall benefits that the programs produce.

NEC has also developed and deployed multimodal biometric solutions that can help improve airport safety during the COVID-19 pandemic. These solutions incorporate both face detection or recognition and thermal sensing technologies that help detect elevated body temperatures among travelers and airport and airline employees. By enabling contactless elevated body temperature detection, identification, and/or identity verification, similar solutions can help employees in other industries safely return to work.

Star Alliance uses NEC’s face recognition technology on a mobile application (the Star Biometrics Hub) and at bag drops, kiosks, membership lounges, and gate boarding. The Star Biometrics Hub (SBH) is an opt-in digital identity platform with robust cybersecurity measures and privacy protections, including limitations on personal data storage and sharing, in compliance with European Union General Data Protection Regulation requirements. With a single enrollment, travelers can use the service with any participating airline and at any participating airport. Because the NEC face recognition algorithm that SBH leverages is highly accurate with face masks, travelers do not have to remove their masks in order to move throughout the airport in a fast, accurate, contactless manner and without showing documents that contain personally identifiable information.

In the entertainment and hospitality industries, amusement parks and entertainment and sports venues use NEC fingerprint and face recognition technologies to facilitate opt-in ticketless entry and VIP access control. By integrating face recognition technologies into exhibits that also use digital touch screens, virtual

3 https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service
5 Of particular significance, on February 6, 2020, the House Committee on Homeland Security held a hearing that explained how the Department of Homeland Security (DHS) is utilizing face recognition technology in Biometric Entry/Exit programs. This hearing followed the December 2019 release of NIST’s FRVT Part 3: Demographic Effects (NISTIR: 8280) report, which provided insight into how different vendors’ face recognition algorithms performed across demographic groups. Witness testimony and Committee questions conveyed several important findings from this NIST report, including that NEC’s algorithm and other top-performing algorithms do not exhibit detectable differences in false positive error rates across demographic groups. Ranking Member Rogers stated, “NIST determined that [the] facial recognition algorithm being adopted by DHS has no statistically detectable race or gender bias.” In other words, NIST could find no statistical evidence that facial recognition algorithms that DHS is adopting contains racial bias.” John Wagner confirmed that “CBP is using an algorithm from one of the highest-performing vendors identified in the report” and that CBP is “not seeing those demographic-based error rates in its deployments.” After the hearing, Chairman Thompson said, “I want to put the safeguards in place so that as we roll out technology we can assure the public that this is not an invasive technology.” He continued, “We’re not prying in folks’ bedrooms. This is strictly a method of identification that helps keep us safe.”
6 On its website, CBP explains its efforts to secure personal data in its biometrics programs through robust requirements for partners who collect data and through CBP’s own data management, including secure encryption and authentication, biometric template protections, brief retention periods, and secure storage practices. https://www.cbp.gov/travel/biometrics/biometric-exit-faqs; https://biometrics.cbp.gov/privacy.
reality technologies, and gesture technologies, NEC helped a museum create a personalized experience for guests who opt in. A beach resort uses our face recognition technologies to give guests who choose to use these technologies the freedom to leave their wallets behind and move through the resort using their faces to access amenities and make payments.

NEC’s state and local government customers use biometric technologies to promote public safety. State departments of transportation and motor vehicles leverage NEC face recognition technologies to compare photos in applications for new or renewed driver’s licenses to existing photo databases, in order to help detect potential attempts to create multiple identities or to use fraudulent identities. These identity theft and fraud detection solutions include a case management system that enables oversight of face recognition technology query results, and we help customers integrate these solutions into more comprehensive processes that include multiple levels of trained human review. State and local law enforcement agencies also use NEC’s Multimodal Biometric Information Systems (MBIS) as tools to query existing state or federal databases to more efficiently and effectively generate leads in criminal investigations. The results from these biometric technology queries do not independently constitute grounds for arrest, and the biometric technologies do not substitute, but rather only support, traditional investigative techniques.

We partner with NGOs, international organizations, and governments around the world to leverage our biometric technologies in ways that help solve societal problems and make progress towards achieving the United Nations Sustainable Development Goals. For example, we collaborated with the United Nations High Commissioner for Refugees and the United Nations Development Programme to provide a refugee registration system and a voter registration system that use NEC fingerprint technologies. In partnership with Gavi and Simprints, we have worked to improve immunization coverage in developing countries around the world by developing and deploying the world’s first scalable fingerprint identification solution that gives children aged one through five a digital ID linked to an accurate, complete medical record. We have also worked with the International Committee of the Red Cross to harness biometric technologies to deliver critical humanitarian aid more efficiently and effectively. Furthermore, we have memorandums of understanding for biometrics projects with other international organizations, including the World Food Programme and the United Nations Industrial Development Organization.

NEC is proud of the benefits that our biometric technologies have brought to communities around the world and of the successful international partnerships that produced these beneficial solutions. We are committed to supporting efforts to help communities worldwide continue to simultaneously benefit from biometric technologies and mitigate the risks that the technologies can pose. Below, we provide more information about biometric technologies, the risks and benefits that biometric technologies can produce in different settings, our ongoing initiatives to promote responsible use of biometric technologies, and biometric technology governance approaches.

II. Biometric Technology Definitions, Functional Applications, and Testing/Validation

Definitions of biometric technologies vary, but commonalities exist across definitions. In general terms, biometric recognition technologies provide an automated means by which to determine an individual’s identity based on the individual’s unique biological characteristic/feature. Many biometric recognition technologies accomplish this task by generating a mathematical representation of an individual’s unique physical attribute (often called a biometric “template”) and then comparing the newly generated template (often called a “probe” template) to one or more templates that are stored in a gallery, in order to determine the degree of similarity between the probe template and gallery template(s). When the biometric recognition technology compares the probe template to a single individual’s gallery template, the technology

---

8 https://www.nec.com/en/global/about/brand/
is performing “verification” (often denoted “1:1 comparison”). When the biometric recognition technology compares the probe template to many or all individuals’ gallery templates, the technology is performing “identification” (often denoted “1:N comparison”).

Many individuals and organizations use the term “biometric technologies” to refer only to biometric recognition technologies, but some individuals and organizations use the term “biometric technologies” to also include biometric detection and biometric characterization technologies. Biometric detection technologies provide an automated means by which to help determine whether a person and/or particular biometric feature is present, without attempting to determine the person’s identity. Biometric characterization technologies provide an automated means of estimating or inferring a person’s emotional state or demographic characteristics based on the person’s biological characteristic(s)/feature(s), but these technologies also do not attempt to identify the person. In this comment letter, we use the term “biometric technologies” to refer only to biometric recognition technologies.

Biometric technology providers store biometric information in the form of biometric templates that are unique to each vendor and product, and vendors employ sophisticated measures to protect biometric templates and promote data privacy and data security. Biometric templates generally contain less information than the original images and audio files do, and biometric templates include data protection measures that prevent restoration of the original image or audio file from the biometric template. Furthermore, unlike a single password that multiple systems may store as the same set of characters, because the biometric template that each vendor/algorithm generates for a given biometric modality is unique, biometric templates for the same biometric feature differ across vendors and products. Therefore, even if a bad actor breached and decrypted the biometric data, the breach would not compromise individuals’ information across all biometric systems. Moreover, similar to the way that vendors can change individuals’ alphanumeric passwords, vendors can change individuals’ biometric templates, which means that individuals would not need to change their physical features in order to mitigate the negative consequences of a biometric data breach.

In large part due to their demonstrated accuracy and the aforementioned privacy and security attributes, a wide variety of users are increasingly interested in leveraging biometric technologies to help facilitate secure and efficient authentication, access control, remote and digital identification, and process automation. In addition to internal testing that companies perform on their own algorithms, independent standards bodies and testing authorities around the world help validate and improve many biometric technologies’ performance. For example, the National Institute of Standards and Technology (NIST) and the U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) organize and direct biometric technology vendor testing of biometric algorithms and full biometric systems, respectively. NIST conducts benchmark testing that evaluates fingerprint, iris, and face verification (1:1 comparison) and identification (1:N comparison) algorithms from vendors around the world. DHS S&T Biometric Technology Rallies test full biometric technology systems’ performance. Vendors also work to build trust

12 See, e.g., https://www.brookings.edu/blog/techtank/2021/05/26/mandating-fairness-and-accuracy-assessments-for-law-enforcement-facial-recognition-systems/ (referring to the face characterization technologies used in the Gender Shades study as “facial recognition systems”).
14 Before selling or deploying new biometric technologies, vendors largely agree that conducting internal and/or external testing to evaluate performance and accuracy overall and across demographic groups and other challenging use cases is crucial. See, e.g., https://www.ibia.org/download/datasets/5741/IBIA%20Ethical%20Use%20of%20Biometric%20Technology%20FINAL.pdf; https://www.securityindustry.org/report/sia-principles-for-the-responsible-and-effective-use-of-facial-recognition-technology/#core.
15 https://www.nist.gov/programs-projects/biometrics
in and validate their biometric technologies by complying with standards from the International Standards Organization (ISO), Organization of Scientific Area Committees for Forensic Science (OSAC) Facial Identification Subcommittee and Facial Identification Scientific Working Group (FISWG), Institute of Electrical and Electronics Engineers (IEEE), American National Standards Institute (ANSI), and similar organizations.

NEC recognizes the importance of validating and improving our biometric technologies’ performance and of contributing to the global development of standards and best practices for biometric technology development, deployment, and use. To do so, we participate in biometric technology standards working groups, work to adhere to relevant biometric technology standards and best practices, and seek out opportunities to submit our biometric technologies to independent, third-party testing. Specifically, to obtain independent evaluations of our biometric algorithms’ accuracy overall and across demographic groups and other challenging use cases, NEC has been participating in NIST vendor tests for well over a decade and in DHS S&T Biometric Technology Rally testing since its inception. We have consistently ranked among the top providers of fingerprint (ranked first eight times since 2003), iris (ranked first twice since 2018), and face (ranked first six times since 2009) recognition algorithms in NIST tests. Most recently, we earned the top rank in NIST’s 2021 1:N iris recognition benchmark test\(^\text{17}\) and the top rank for identifying individuals in law enforcement mugshot photos and border images (10+ years) in NIST’s 2021 1:N face recognition benchmark test.\(^\text{18}\) NEC face recognition technologies also were the most accurate at identifying individuals both wearing and not wearing face masks in DHS S&T’s 2020 Biometric Technology Rally.\(^\text{19}\)

III. **Biometric Technology Benefits, Risks, and Risk Mitigation Approaches**

The risks and benefits that biometric technologies can produce differ based on the biometric modality and functional application selected and the setting and way in which users deploy the technologies. Technology vendors; end users; other privacy experts; and federal, state, and local government entities have developed strategies and techniques to help mitigate many of the risks that biometric technologies can pose, but continued policymaker and multi-stakeholder risk mitigation efforts would be helpful.

**A. Different biometric technology modalities and functional applications can create different opportunities and challenges across use cases.**

The industry widely recognizes several biometric technology modalities, including face, iris, voice, fingerprint, palm print, latent print, tenprint, finger vein, ear acoustic, and gait.\(^\text{20}\) Many also consider DNA and predictive genotyping technologies to be biometric technologies.\(^\text{21}\) Generally, the more unique and consistent a biological feature is, the more accurate of an identifier that feature is. For example, an individual’s DNA sequence is very unique and stays consistent over time. In contrast, an individual’s gait is less unique and consistent over time. However, even the most accurate identifiers are not only or always the best choice for a given use case, and different modalities create distinct benefits and risks.

The visibility of the biological feature; the ease, speed, comfort, and cost of gathering information about the biological feature; and other considerations can impact whether or not a biological feature is an appropriate modality candidate for a given use case. For example, people’s faces are highly visible in public, and taking photos of individuals’ faces is relatively easy and inexpensive to do and can occur at a distance and in a contactless manner. On the other hand, people’s fingerprints are not as visible in public, and capturing individuals’ fingerprints can be challenging at a distance and/or without requiring individuals to make contact with or get very close to a surface or object. Due to these differences, biometric technologies that help identify individuals based on their faces may be more useful in settings where contactless

---


\(^\text{20}\) [https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/](https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/)

\(^\text{21}\) [https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/](https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/)
identification is a priority. Where contactless identification is less of a priority and where environmental conditions make capturing high-quality face images difficult, biometric technologies that help identify individuals based on their fingerprints may be more useful.

i. Modality-Specific Risks Related to Enabling Unlawful Ongoing Surveillance

Different biometric technology modalities and functional applications also pose different risks, including privacy and broader civil rights and civil liberties risks related to enabling unlawful ongoing surveillance. For example, because capturing fingerprints in real time requires a person to touch or get very close to a specific object and cannot easily occur at a distance, fingerprint technologies, such as those that many people use to unlock devices and access secure facilities, are unlikely to infringe on individual privacy by enabling unlawful ongoing surveillance. At the same time, having many individuals come into close contact with the same objects could contribute to the spread of infectious diseases, like COVID-19. Iris and voice recognition technologies do not necessarily require an individual to touch an object, but they are not effective at significant distances. Plus, iris recognition technologies require individuals to look directly at a specific point under specific lighting conditions, and voice recognition technologies are less effective when background noise is present. Therefore, iris and voice recognition technologies are unlikely to enable unlawful ongoing surveillance in public spaces or crowded private spaces.

Face recognition systems that require an individual to take a photo at a kiosk, such as those that enable contactless payment and contactless access control, require active user engagement and do not capture an individual’s biometric information at a great distance or on an ongoing basis. Therefore, these face recognition systems are also unlikely to contribute to unlawful ongoing surveillance. In contrast, if misused, real-time video monitoring face recognition (and, in particular, identification) solutions could enable unlawful ongoing surveillance because these technologies could potentially enable users to identify and track individuals in real time, at a distance, and without the individuals’ awareness. However, these same real-time video monitoring face identification solutions can help perform tasks like identifying missing and exploited children and human trafficking victims in security camera footage.

These examples illustrate that some modalities and functional applications pose greater risks of enabling unlawful ongoing surveillance than other modalities do. Yet, the same modalities and functional applications that could enable unlawful ongoing surveillance can also support lawful public health and safety efforts. Consequently, as we explain in more detail below, to simultaneously protect privacy and reap the benefits that biometric technologies can produce, taking a tailored approach to risk mitigation that differentiates between modalities and functional applications is important.

ii. Risks Related to Perpetuating Harmful Bias

Policymakers and media outlets have been increasingly focused on investigating and addressing ways in which biometric technologies could potentially perpetuate harmful impacts of bias. We appreciate the focus on this important issue and are dedicated to working with other stakeholders on initiatives that aim to ensure that the use of biometric technologies helps advance racial and broader social justice. Biometric technology bias issues are multifaceted and complex, and they vary across functional applications and use cases, but they generally fall into two main categories: (1) technical issues in the biometric technologies that produce inconsistent performance across demographic groups and (2) ways in which the use of biometric technologies can perpetuate bias in society.

Any biometric technology modality can exhibit bias by performing differently across demographic groups, and several components of biometric technologies can contribute to these demographic performance differences. One such component is the biometric algorithm. For example, NIST’s December 2019 FRVT

---


Part 3: Demographic Effects (NISTIR: 8280) report found that many face recognition algorithms do exhibit significant differences in performance across demographic groups and exhibit lower accuracy rates for darker-skinned women than lighter-skinned men. However, this report also found that several algorithms, including NEC’s, had “undetectable” false positive error rate differences across demographic groups and that NEC’s algorithm had the lowest false negative demographic differential.

The capture device is another component of the biometric technology system that can impact system performance across demographic groups. If capture devices, such as cameras, fingerprint scanners, iris scanners, and sound recording devices, generate poorer quality probe images or audio files for individuals who are members of particular demographic groups, these devices can contribute to lower accuracy rates across those demographic groups. Further research into capture device performance across demographic groups and the ways in which capture device quality impacts biometric technologies’ operational performance would be helpful, but DHS S&T has already done commendable work evaluating certain biometric technologies’ full system performance. As we mentioned above, NEC has consistently ranked among the top technology vendors in DHS S&T Biometric Technology Rally tests, most recently achieving face recognition technology accuracy rates of >98% with face masks and >99% without face masks.

Questions about face recognition technologies’ performance across demographic groups have received the most media and policymaker attention in recent years, but other biometric technologies have encountered and overcome demographic performance issues as well. For example, fingerprint technologies did not always perform consistently across racial groups and have historically struggled to identify very young children due to the small size and limited development of child fingerprints. Nonetheless, NEC’s partnership with Gavi and Simprints provides a practical example of how fingerprint technologies have advanced enough to accurately identify one-year-olds who are members of diverse racial groups.

Using inaccurate biometric technologies has the potential to perpetuate bias and inequity in society. Technologies that do not perform accurately overall and across demographic groups can reinforce the harmful impacts of bias by contributing to more frequent misidentifications of individuals who are members of marginalized groups. Without adequate oversight and mitigation, these misidentifications can contribute to processing delays, unnecessary contact with law enforcement officials, and other negative experiences for individuals who already face disproportionate challenges and barriers in our society. Conversely, when used appropriately, biometric technologies that perform highly accurately overall and across demographic groups can help reduce the harmful impacts of bias by making identifications more accurate.

Furthermore, because biometric technologies compare templates without making assumptions about an individual’s demographic characteristics, highly accurate biometric technologies can act as a check on inherent biases that often contribute to misidentifications, including in high-stakes criminal justice settings. Nonetheless, even biometric algorithms that are highly accurate overall and across demographic groups can perpetuate biases when they increase the speed and accuracy of processes, institutions, and systems that produce biased outcomes. Considering and addressing the impact of biases in processes, institutions, and systems are important elements of multi-stakeholder efforts to support ethical use of biometric technologies.

B. The risks and benefits that each biometric technology modality and functional application can produce vary across use cases.

Using biometric technologies to aid in identification and identity verification tasks creates different degrees of risk in different settings. Generally, higher-risk use cases are those in which the use of biometric technologies substantially contributes to decisions that most significantly impact civil rights, civil liberties, and/or human rights. Because accurately identifying individuals (or verifying their identities) is especially

important in these use cases, using biometric technologies in ways that improve identification and identity verification accuracy, including as part of processes that incorporate trained human review and other safeguards, can also be especially beneficial.27

Although commercial uses, and especially uses pertaining to healthcare systems, financial institutions, and payment systems, can pose risks that are important to consider and address, public-sector uses of biometric technologies can create higher risks. Within the public-sector, law enforcement uses of biometric technologies tend to pose the greatest risks, followed by use cases that deal with access to essential government services, like driver’s license applications and benefits administration. Law enforcement use of real-time video monitoring face recognition technologies is widely regarded as the highest-risk potential biometric technology use case. Regardless of who does the tracking, automatically tracking an individual’s location and monitoring an individual’s behavior from a distance and potentially without the individual’s consent or awareness could be concerning from a privacy and broader civil rights perspective. If law enforcement agencies are the ones using real-time video monitoring face recognition technologies, the automated tracking and monitoring could contribute to an individual’s arrest and, later on, incarceration. This makes law enforcement use of these technologies particularly high-risk. Because other identifications in law enforcement settings, such as those that help generate investigative leads, can also contribute to arrest decisions, such use cases are also relatively high-risk and require additional policy safeguards to mitigate unintended consequences.

IV. NEC Promotes Responsible Use of Biometric Technologies through Our Commitment to Building Digital Trust and Upholding Our AI and Human Rights Principles

NEC Corporation’s Digital Trust Business Strategy Division (DTBSD) works with multiple corporate functions on several environmental, social, and governance (ESG) initiatives.28 Key among those ESG initiatives are ongoing efforts to formulate and implement a strategy for promoting human rights in our biometrics and broader AI business. In 2018, DTBSD leveraged internal and external expert perspectives to develop the NEC Group AI and Human Rights Principles, which promote: (1) fairness; (2) privacy; (3) transparency; (4) responsibility to explain the effects, value, and impacts of AI utilization; (5) proper utilization of AI technology; (6) continued development and improvement of AI technologies; and (7) dialogue with multiple stakeholders. We are committed to upholding our AI and Human Rights Principles through corporate governance initiatives, product risk management practices, customer and partner relationship management approaches, and internal and external multi-stakeholder engagements.

One global corporate governance priority that helps operationalize the Principle of privacy is continuing to update and comply with the NEC Corporation Privacy Policy and our personal information protection management system requirements. Both our Privacy Policy and our personal information protection management system mandate handling personal information in accordance with applicable laws and relevant industry standards, including the requirements in Japan’s Act on the Protection of Personal Information and JIS Q 15001, the Japanese industrial standard for safe and appropriate management of personal information in corporations’ and other organizations’ operations. We have also implemented data breach response procedures to help ensure that, if a data breach does occur, we are well positioned to respond effectively and in a manner that minimizes harm to the individuals whose personal information we retain. In recognition of these efforts, we have been PrivacyMark-certified for many years and first earned our certification in October 2005.29 As of March 2021, NEC Corporation and thirty of our affiliated companies hold the PrivacyMark certification.

29 To earn the PrivacyMark certification, companies must comply with JIS Q 15001 and gain third-party organization recognition for having systems in place to ensure appropriate protection measures for personal information. The PrivacyMark certification also prohibits companies from collecting information that could economically impact an employee, such as bank account and
To develop, manage, and improve other policies, programs, and practices as part of our global human rights promotion strategy, DTBSD consults diverse experts from around the world about human rights issues relevant to our business and to the communities in which we operate. DTBSD also collaborates with other internal teams worldwide, including the People and Organization Development Division, global quality management and cybersecurity teams, and regional subsidiary teams that are working to build digital trust in their local markets. One such regional subsidiary team is the U.S.-based Digital Trust Initiative (DTI), which takes a three-pillared approach to building digital trust by promoting (1) reliability, (2) ethics and human rights, and (3) security in our business practices, services, and technologies. One of DTI’s top priorities is continuing to operationalize the NEC Group AI and Human Rights Principles in our U.S. biometrics business.

In our biometrics business, we uphold the NEC Group AI and Human Rights Principles in our approaches to product design and development, customer and partner screening, product deployment, and customer support and training. Throughout the process of designing and developing our biometric technologies, NEC leverages safeguards such as encryption (including homomorphic encryption30), data minimization, data aggregation, data anonymization, and algorithm layering. We also test our biometric technologies’ performance internally and submit our technologies to third-party testing authorities, like NIST and DHS S&T, to verify that our technologies perform accurately overall and across demographic groups. Before selling our highest-risk biometric technology solutions through new partners and/or to new customers, we believe that considering the prospective partners’ and customers’ human rights records and risk mitigation policies is important. We aim to sell only through trusted partners and to trusted customers, and we are willing to decline business opportunities that we determine may pose too great a risk to human rights. After we decide to sell a biometric technology solution to a customer, we work with the customer (and, if applicable, the partner(s)) to plan and execute deployments and to train individuals operating the biometric technology systems on proper use. We recommend that customers adopt use policies that require safeguards, such as appropriate human review of query results and continuous system performance monitoring, and we provide system operators with ongoing support via a customer service helpline and field site visits. We also work with our partners and customers around the world to facilitate multijurisdictional legal compliance (including by completing privacy impact assessments) and to consider ethical issues that may arise in the context of customers’ biometric technology deployments. Our consideration of these ethical issues reflects perspectives gained through collaboration with diverse internal and external stakeholders.

Internally, we are actively working to strengthen human rights literacy and to promote diversity, equity, and inclusion (DEI) throughout NEC, and particularly on our biometrics and broader AI teams. In addition to providing training programs and advancing other education and information sharing initiatives, we recognize the importance of continuing to deepen collaboration between our DEI Steering Committee, our Digital Trust Initiative, and our broader product and leadership teams. This collaboration will help NEC more completely embed our commitments to DEI and social justice into our policies, programs, and practices for designing, developing, deploying, and evaluating our biometric and other AI technologies.

To inform our perspectives and positions on issues at the intersection of biometric technologies and civil and human rights, we also participate in dialogues with a wide array of external stakeholders, including policymakers, civil society organizations, think tanks, industry groups, end user groups, and academic and government researchers around the world. We welcome opportunities to serve as a resource to policymakers

30 “Homomorphic encryption for biometric matching holds the promise of data protection even in use, and NEC Corporation is the latest technology provider to develop a system that it says delivers on this promise, with the key difference that the company says it can be used for one-to-many searches. Biometric data encrypted between collection and transmission to a server or service provider for matching prevents the leakage of raw images, which can be subsequently utilized in spoofing attacks. In the system developed by NEC, the decryption key is held by the user, rather than the service provider, providing users with additional assurance their information is protected.” https://www.biometricupdate.com/202112/nec-streamlines-1n-biometric-matches-for-homomorphic-encryption-to-protect-data; see also https://www.nec.com/en/press/202112/global_20211216_02.html.
and other stakeholders who are interested in learning more about biometric technologies and developing approaches to mitigating biometric technology risks while realizing biometric technology benefits.

V. **Policymakers Can Develop Governance Frameworks to Promote Responsible, Trustworthy Use of Biometric Technologies**

Developing governance frameworks that promote privacy and other civil rights and civil liberties, racial and broader social justice, safety, security, economic efficiency, and technological innovation requires a nuanced analysis and approach to regulating different types of biometric technologies in different settings.

Many of the biometric technology governance principles, frameworks, and recommendations that technical experts, government agencies, privacy professionals, and scholars have developed require strong cybersecurity protections; appropriate and feasible notice and consent to the use of biometric technologies and related data collection; limitations on data handling, storage, retention, and transfer; both internal and independent, third-party testing before and after deploying biometric technology systems; operator training; public reporting and oversight to the degree appropriate for various use cases; meaningful human review of high-stakes biometric technology query results; prohibitions on discrimination in decision-making based on biometric technology query results; and other use limitations that ensure existing constitutional protections appropriately demarcate uses of biometric technologies in the United States. Although these types of requirements are common across numerous proposed governance principles and frameworks, the specific details of each requirement vary based on the risk associated with each biometric technology modality, functional application, and use case.

In addition to establishing requirements for the use of biometric technologies, policymakers can develop governance frameworks that promote transparent government procurement and deployment of high-quality, regularly upgraded biometric technology systems. These governance frameworks can also support continued biometric technology research by NIST, DHS S&T, academic institutions, and public-private partnership teams. Such research should address topics such as the performance of full biometric technology systems and particular system components across demographic groups, risk mitigation strategies for biometric technology design and deployment, operational testing of biometric technologies to evaluate accuracy both overall and across demographic groups, and best practices for human operation of biometric technologies and human review of biometric technology query results to promote accuracy and to identify and overcome any bias.

VI. **Closing**

We recognize that, due to space constraints, our comments in this letter only begin to address the complex issues that OSTP’s RFI raised. We would welcome future opportunities to discuss the risks and benefits that biometric technologies can produce and potential biometric technology governance approaches in greater depth. In particular, we would be interested in participating in working groups and/or multi-stakeholder dialogue sessions that specifically address particular biometric technology use cases, modalities, and/or functional applications.

Sincerely,

Shin Takahashi
Chairman and Head of Government Relations and Public Policy

---