January 4, 2022

To: Office of Science and Technology Policy
Executive Office of the President

Via electronic mail

From: Elizabeth M. Renieris, *Professor of the Practice, Director of Policy, Notre Dame Technology Ethics Center* and Yong Suk Lee, *Assistant Professor of Technology, Economy and Global Affairs, Faculty Affiliate, Notre Dame Technology Ethics Center*[*]

Re: *RFI Response: Biometric Technologies*

We are colleagues at the University of Notre Dame's Technology Ethics Center, which develops and supports multi- and interdisciplinary research on questions related to the impact of technology on humanity. We are writing in response to the White House Office of Science and Technology Policy's request for information on "Public and Private Sector Uses of Biometric Technologies" as part of its broader efforts to develop a Bill of Rights for an Automated Society. In summary, the already widespread and rapidly proliferating use of biometric technologies across the public and private sectors raises a wide array of ethical concerns and challenges. As such, we are encouraged by the OSTP's efforts to consider policies that can equitably harness the benefits of these technologies while providing effective and iterative safeguards against their anticipated abuses and harms.

Our response is focused on use cases (topic 1) and harms (topic 4), as set out below:

1. Descriptions of use of biometric information for recognition and inference: Information about planned, developed, or deployed uses of biometric information, including where possible any relevant dimensions of the context in which the information is being used or may be used, any stated goals of use, the nature and source of the data used, the deployment status (e.g., past, current, or planned deployment) and, if applicable, the impacted communities.

UNITED STATES

- *Biometric IDV*
  One of the most common uses of biometric technologies at present is in the context of digital identity and access management (IAM), including for identity verification

[*] We would also like to acknowledge Benjamin Larsen, a PhD Fellow at the Copenhagen Business School and The Chinese Academy of Sciences (CAS) in Beijing, for his significant research contributions on use cases.

(IDV) and authentication. Verification is typically a one-time process used to onboard a customer or create an account for an individual by linking a unique individual to an identity document or other identity information. Authentication is typically a recurring process by which to determine that a previously verified individual is who they say they are on the basis of one or more factors of authentication. Low assurance environments (e.g., social media accounts) may require simple login credentials such as a username and password, while higher assurance ones (e.g., a benefits portal) may require two or more factors such as login credentials and a code sent to a verified phone number associated with the account. Even higher assurance environments (e.g., bank accounts) increasingly require physical biometrics, such as fingerprints, faceprints, voiceprints, iris or retina scans, and behavioral biometrics, such as keystroke dynamics, eye-tracking, and gait recognition, among other modalities.

Emerging technologies such as artificial intelligence (AI) and machine learning are increasingly used to process biometrics for IAM purposes. For example, remote, AI-powered IDV through the use of biometric facial verification allows individuals to prove their identity by providing an image of an identity document (e.g., a driver's license) and a live picture or video of their face. Machine learning models are then used to determine the likelihood that the document is authentic by extracting data from it and attempting to detect any manipulations. If the document is deemed authentic, the model is used to perform a biometric-based facial similarity check to determine whether the image on the document matches the face in the selfie or live video of the individual presenting it. If the faces match, the person passes the IDV check.

Beyond AI-powered IDV, here are other examples of private sector use cases in the U.S.:

- *Contactless Payments/Checkout*
  Biometrics are increasingly embedded into "contactless" payment and checkout solutions. For example, restaurants are beginning to use facial recognition technologies (FRT) for contactless drive-thru orders and payments through companies such as PopPay. While there has been significant emphasis on the use of FRT, a wide array of other physical and behavioral biometrics is also increasingly being used by the private sector for payments. For example, Amazon One uses vein scanning technology to turn an individual's palm into a physical biometric that can be used for contactless checkout in its Amazon Go grocery stores. Payment providers like Mastercard and Visa are also beginning to embed vein scanning and fingerprint recognition technologies into their payment solutions. Proponents argue these biometric-enabled tools make these processes more efficient, convenient, and secure, and uptake has been boosted in part by pandemic-induced germaphobia.

- *Exam Proctoring/Remote Learning*
  As many educational activities have shifted online during the pandemic, there has been a considerable increase in the use of remote learning software and remote proctoring tools to administer exams. Companies like Proctorio, ProctorU, and Honorlock purport to use a variety of behavioral biometrics, such as gaze-detection and eye-monitoring, face-detection and head movement tracking, and mouse clicks and scrolling patterns, among other behaviors, to detect cheating or other abnormalities during exams. These tools presume there are "normal" behaviors or patterns and that deviations or "abnormal" movements indicate cheating or fraud.

- *Security/Loss Prevention*
  The use of FRT among U.S. retailers for purposes of security, theft or loss prevention is already a widespread practice and includes household names such as Apple, Lowe's, and Macy's, among others. Going beyond facial recognition technologies, retailers are increasingly adopting invasive biometric methods and modalities, many of which were initially developed by the Pentagon, that purport to use things like heart rate (or "cardiatric signature"), body odor and other chemical indicators, gait analysis, and more to predict theft or other criminal activity in stores.

- *Employee Monitoring/Tracking*
  Employers are increasingly using AI-powered biometric systems to monitor, track, and nudge employees into certain activities or behaviors. For example, Amazon delivery drivers have to sign "biometric consent" forms to allow biometric sensors to collect facial images and other biometric information in the name of driver "safety." Wearables and biometric-enabled sensors are increasingly being considered to monitor and surveil employees for social distancing and other pandemic-related protocols.

Biometrics are also increasingly part of public sector use cases, such as the following:

- *Policing/Law Enforcement*
  Police and law enforcement agencies frequently use a variety of facial recognition software tools in their efforts to identify both suspects and victims, otherwise solve crimes, and, increasingly, to police certain neighborhoods. Some uses are less targeted and involve more pervasive surveillance and monitoring of specific communities (typically lower income and minority communities). Often, these tools are provided by private sector firms, such as the controversial Clearview AI whose database allegedly contains nearly 3 billion facial images.

- *Education/Schools*

In addition to remote learning tools, public schools and universities are increasingly adopting technologies that incorporate an array of physical and behavioral biometrics for various purposes on school premises. For example, during the pandemic a number of schools and universities began using fingerprint readers for contactless ordering and payments in dining halls and cafeterias. Facial recognition systems and behavioral biometric-based systems are also being explored for school safety and security purposes, including, in some cases, to replace metal detectors.

- *Security/Access Control*
  Public sector entities were early adopters of the use of fingerprints and other physical biometrics for purposes of security and access control. In part due to the pandemic, DHS and the TSA are increasing their investment in facial recognition systems, including iris scanners and other biometric-enabled technologies to automate a variety of processes in airports and other travel hubs, from security and passenger screening to check-in, health checks and other COVID-19 related protocols. Here, it is important to reiterate the public sector's increasing dependence on private sector provided tools. For example, DHS has moved its biometrics database to Amazon's cloud service.

CHINA

While the use of biometric technologies in the United States is widespread and rapidly accelerating, in large part due to the COVID-19 pandemic, these technologies are also ubiquitous in other countries, where certain use cases may foreshadow what is to come. For example, China has been aggressively using biometric technologies for purposes of convenience, safety, and surveillance in both public and private sector contexts. New wearable devices such as "smart" helmets, "smart" bands, and "smart" uniforms are increasingly being used by organizations in an attempt to detect individuals' movements and whereabouts, as well as changes in their emotional states. The wireless sensors of "smart" helmets, for instance, constantly monitor the wearer's brainwaves and stream the data to computers that use AI algorithms to purportedly detect emotions such as depression, anxiety, or rage, as well as other mental activities, which, can purportedly be monitored or used to prevent accidents or increase safety or efficiency in an organization.

Here are some more specific examples of private sector applications in China:

- *Helmets – Manufacturing Company*
  Manufacturing firms are outfitting their workers to wear caps that can monitor their brainwaves. Management seeks to use this data to adjust the pace of production and redesign workflows. For example, Hangzhou Zhongheng Electric believes it could increase the overall efficiency of the workers by manipulating the frequency and length of break times to reduce the mental stress of workers.

- *Cushions –Tech Company*
  Hebo Technology, a private firm in Hangzhou, developed and gave smart cushions to its employees. The smart cushions alert managers when employees appear to be away from their desks, or when an employee appears to get emotional or stressed. Smart cushions are additionally being used to monitor an employee's vital signs, which also informs workers when to get up and stretch. Companies can use this collection of data to cross-reference it with an employee's general performance at work.

- *Bands/Uniforms - Service Company*
  A sanitation company use smart bands to keep track of idle workers, and send out alerts saying "please continue working, add oil!" if there has been no movement from the wearer for more than 20 minutes. Smart bands and smart uniforms embedded with ID chips and GPS function are being used to monitor location and to keep track an employee's whereabouts. The devices are also used as a way for workers to clock in, and ensure they remain in their designated work areas, which management uses to potentially increase efficiency and lay off lazy workers.

And here are some more specific examples of public sector applications in China:

- *Helmets – Hospitals*
  Hospitals use smart helmets to allegedly monitor patients' emotions and prevent violent incidents. In addition to the helmet, a special camera captures a patient's facial expression and body temperature, while pressure sensors under the bed monitor shifts in body movement. Together, it is believed that the collected information can give a more precise estimate of the patient's mental status. Patients are informed if their brain activities are monitored, and the hospital does not activate the devices without the patient's "consent" (the sufficiency of which is another matter).

- *Helmets - High-speed Trains*
  Brain monitoring devices are worn regularly by train drivers working on the Beijing-Shanghai high-speed rail line. The sensors, built in the brim of the driver's hat, are purportedly used to measure various types of brain activities, including fatigue and attention loss with an accuracy of more than 90 percent, according to the company's website (e.g., if a driver dozed off the cap could trigger a cabin alarm to wake him up).

- *Headsets – Public Schools*
  Some schools have made students wear brain-wave sensing gadgets that can purportedly help track their attention and concentration-levels during class. The idea is that teachers can access this data to track who is paying attention or not, and that parents can also track their kids' attention levels and compare them with the scores

and grades of other kids in class. Teachers say the students pay better attention after wearing the devices, which makes them more likely to study harder and obtain better scores. Data collected can also be repurposed for government-sponsored research.

- *Bands/Uniforms - Public Schools*
  A secondary school in Guangdong uses Tencent's smart campus platform and smart bands to monitor the location of students, the number of people in the area, class arrivals, and campus entry and exit information, which can be paired with FRT to monitor students, staff or unwanted individuals around campus. Tencent's smart campus platform has already been deployed at more than 300 schools and universities and is alleged to give school management, teachers, and parents a way to obtain more information about the students and their activities.

4. Exhibited and potential harms of a particular biometric technology: Consider harms including but not limited to: Harms due to questions about the validity of the science used in the system to generate the biometric data or due to questions about the inference process; harms due to disparities in effectiveness of the system for different demographic groups; harms due to limiting access to equal opportunity, as a pretext for selective profiling, or as a form of harassment; harms due to the technology being built for use in a specific context and then deployed in another context or used contrary to product specifications; or harms due to a lack of privacy and the surveillance infrastructure associated with the use of the system. Information on evidence of harm (in the case of an exhibited harm) or projections, research, or relevant historical evidence (in the case of potential harms) is also welcome.

These use cases present a wide array of known and potential harms and ethical concerns.

1. Ethics of Biometric IDV Systems

To be reliable and accurate, biometric digital ID solutions require a lot of data—typically sensitive, personal data such as facial images and other biometrics. For example, a training set of millions of faces is required for AI facial similarity checks, which are only as good as the training data and require continuous monitoring and correction of the model. Mistakes in AI used for biometric IDV can lead to significant consequences, such as the denial of access to services, especially when there is no analog or physical alternative, which is increasingly the case. This challenges traditional data protection and privacy principles such as data minimization, purpose and use limitations, storage limitations, transparency and accountability requirements, and data integrity and quality principles, among others, while introducing new risks of bias, discrimination, and exclusion.

While we tend to focus on the data privacy and security features of a specific AI-powered biometric technologies, we typically ignore the privacy and security implications for people whose personal data, faces, and other biometrics are used to build and train those tools and models in the first place. As a result, there is an asymmetry between the privacy of individuals used to build and train the AI and the beneficiaries of any tools ultimately built and deployed from those data sets. Moreover, as a result of complex supply chains of personal data use, the entities designing and building AI-based identity solutions are often not the ones using or deploying them. Without a direct relationship to the companies designing and building these tools, the chain of responsibility and accountability for privacy and security often breaks down, leaving individuals with limited visibility, control, or recourse over how their information is used.

2. Shaky Scientific Foundations

Many of the use cases for physical and behavioral biometrics described herein are based on controversial or shaky scientific foundations. It is widely recognized that general FRT systems are prone to bias based on gender, race, ethnicity, age, and other characteristics. Other physical biometric modalities such as voice recognition have been shown to exhibit similar biases. Many tools and technologies that incorporate physical and behavioral biometrics assume that it is possible to automatically and systematically infer certain emotions or other internal states or proclivities of human beings from outwardly observable features, expressions, movements, or behaviors, without a solid scientific basis. For example, as FRT is increasingly used for emotion detection or to predict certain behaviors or traits, we must recognize that things like facial expressions vary widely across cultures and contexts, making such systems inherently suspect.

Similarly, other physical and behavioral biometrics, such as gesture recognition or gait analysis, presume some kind of “normal” from which deviations are deemed “abnormal” and indicative of certain traits of proclivities. These systems are inherently discriminatory against individuals with differences in body shape, posture, mobility, or certain disabilities, and can exacerbate the risks of inequitable treatment and exclusion.

3. Data Privacy Concerns

In the United States, the lack of comprehensive federal privacy legislation means that many uses of data implicated in these biometric technologies remains largely unregulated. While some states have passed privacy legislation, these laws often fail to adequately address the kinds of biometrics implicated in many of these systems. Even Illinois’ Biometric Information Privacy Act, which regulates the collection, use, and handling of biometric identifiers by private entities, and is arguably the most stringent biometrics law in the country, narrowly defines “biometrics” such that it would not cover a wide array of new modalities of behavioral biometrics and is easily bypassed by “consent.”

Over-collection of data as well as predatory data-gathering practices is also very common in China, since regulation on the areas has historically been laxer, trailing behind the EU, for example. New regulation such as the incoming Personal Information Protection Law (PIPL) is changing this, however, and large companies have already altered and strengthened their data gathering and data privacy practices considerably. With respect to over-collection of data, it is not clear whether people are genuinely appeased by stronger measures taken with regards to China's private sector enterprises, whereas extensive collection of data by the state, is simply an area to be accepted and respected, similarly to the legitimacy of the CCP.

The Chinese government has directed large Chinese companies such as Alibaba, Baidu, ByteDance, Xiaomi, Pinduoduo and Meituan, to rectify a number of issues on their apps, such as mishandling of personal data, frequent harassment of users, and deceiving consumers to give up more of their data including through the use of "dark patterns." Smaller companies have also been directed to rectify a number of similar issues on their apps. Companies use personal data for consumer profiling, which allows for more targeted commercials and advertisements. Data may also be sold in markets for data, which makes small companies engage in predatory practices to collect large swaths of individual data, and generally more data than the company needs for its app itself. Large companies can benefit considerably as they have access to big swaths of individual data.

Chinese citizens are increasingly becoming aware and concerned of data privacy issues. Baidu has, for example, been brought to court in the city of Nanjing by a government-controlled consumers' group. The group claims that a Baidu app illegally monitors users' phone calls without telling them. Ant Financial, which is the financial arm of Alibaba, the country's largest e-commerce group, has also made a public apology for a default setting on its mobile-money app, which automatically enrolled customers in a credit-scoring scheme, called Sesame Credit, without their active consent. If companies are able to monetize consumers' private data, they have an incentive to over-collect personal data and thereby infringe on user privacy.

4. Data Security/Cybersecurity Concerns

While data leaks and cybersecurity issues are as common and concerning in China as they are in the U.S., Europe, and elsewhere, China's strong emphasis on rapid technological implementation and experimentation means that many technologies may overlook or neglect security aspects, particularly as fines for security breaches remain insignificant. New and incoming laws are changing this, however. It is unclear whether people care more about data leaks by public sector agencies (e.g., FRT, school-platforms and wearables) or by private sector entities, which could reveal relative attitudes towards public versus private sector technological implementation and measures of surveillance.

FRT in Residential Neighborhoods & Schools. Residential neighborhoods and apartment complexes across China are rapidly adopting FRT, accelerated by Covid-19. However, incorrectly configured databases remain a widespread security problem in China, as tech companies and workers implement certain technologies too quickly without taking the necessary data security or cybersecurity precautions. As a result, personal data is often insecure and easily leaked. Similar problems are arising in schools. For example, a middle school database in China full of photos of students' faces, ID and student numbers, and GPS locations, was recently left open to the internet without any encryption or other protections. It contained records of 1.3 million people, including students, teachers, cleaners and security personnel, with great risk that individuals' data will be misused.

5. Government Surveillance

As noted above, FRT systems have garnered significant attention and controversy, largely due to concerns about pervasive and expanding government surveillance. Cities and municipalities across the U.S. are imposing limits on the use of FRT, going so far as to ban the technology outright through statewide moratoria in Vermont and Virginia, and in cities including Berkeley, Oakland, and San Francisco in California; Portland, Oregon and Portland, Maine; Boston, Cambridge, Somerville, and other cities in Massachusetts; Minneapolis, Minnesota, and more. But just as these bans were gaining momentum, the shift to a more digital existence during the COVID-19 pandemic, including the proliferation of digital contact tracing, exposure notification, proof of vaccination and health status, and other apps has accelerated and normalized the presentment of biometrics.

In China, the government supports a range of new data-gathering technologies to improve public goods such as safety and health. This includes FRT, which gather individuals' biometric information through surveillance of public spaces. For example, when buying a sim-card, individuals are also required to give up their biometric facial data, which is gathered in order to purportedly combat fraud or abuse. Many public schools are being surveilled, and it is believed that tracking students is a measure to increase safety. Along with the construction of the social credit system which can allegedly help to reduce fraud and criminal behavior, the government is able to keep track of individuals. However, the boundary between public good purposes and government surveillance remains murky.

6. Perverse Incentives

Digital identity is big business and growing bigger each day. The global market for IAM is expected to reach $29.79 billion by 2027, while the global IDV market is expected to reach $17.8 billion by 2026. Cloud-based authentication or identity-as-a-service based on AI/ML is one of the fastest growing market segments. ID products and services are typically either enterprise grade (B2B) or consumer grade (B2C). For example, the entity building a remote, AI-based IDV tool is typically a vendor to another company providing a product or service to end users. A common business model in B2B arrangements is a *pay-per-verification* scheme, whereby the AI vendor is compensated per verification check (per query or API call) or per user in a given time frame (e.g., one month). Alternative subscriptions, volume-based pricing models, and hybrid arrangements also exist.

When we move through the physical world, we are rarely asked to identify ourselves. Presenting a government-issued ID is the exception, reserved for high-risk situations like boarding an international flight. But as the market for digital ID systems and solutions grows larger, and as everything from online to in-person services increasingly has a digital component, we are at risk of flipping that paradigm and of requiring people to identify themselves in every setting. Increasingly cheap, efficient, and “seamless” forms of biometric-enabled ID, such as contactless payments and palm scanning technologies, could create a fictious need for individuals to identify themselves in contexts where such a need did not exist before. We risk going from ID as the *exception* to ID as the *rule,* especially if we fail to address the nature of the business models of these schemes.

There are few commercial incentives around the use of your physical, government-issued ID documents. In general, no one gets notified or paid when you use them (e.g., the DMV isn’t typically notified or paid when you use your license to purchase alcohol). In contrast, digital ID schemes have commercial and technical incentives that are very different from in-person, manual processes. Commercial arrangements such as *pay-per-verification* schemes could incentivize the overuse of ID tools and further normalize the presentment of biometrics. Additionally, the use of AI and ML in combination with biometrics for digital ID management risks transforming identity from something *relational* (established in the context of government to citizen, or business to customer) into something *transactional.*

CONCLUSION

In sum, biometric technologies are already widespread in both the public and private sectors throughout the United States, as they are in other countries, such as China. While FRT has been a primary focal point of the conversation, a wide array of other physical and behavioral biometric modalities present similar concerns with respect to ethics, shaky scientific foundations, data privacy and security, the risks of government surveillance, and perverse business models that risk commercializing all of our interactions, whether as citizens, employees, or consumers. We hope the use cases and harms outlined above help to inform the OSTP as you develop a Bill of Rights for an Automated Society. Should you have any additional questions or concerns about our response to this RFI, please do not hesitate to contact us via email at erenieri@nd.edu or yong.s.lee@nd.edu.