Statement to PCLOB by Jason Matheny

Commissioners and attendees, it's a privilege to be here. My name is Jason Matheny. I'm the director of a new center at Georgetown University focused on security and emerging technology, a Commissioner on the National Security Commission on Artificial Intelligence, and a member of the Intelligence Community Studies Board of the National Academies. I was formerly the Director of IARPA, an organization within the federal government that funds breakthrough technologies for national intelligence. I'm going to spend a few minutes describing emerging technologies that are likely to affect privacy in the next two decades.

I'll begin by listing emerging technologies likely to reduce privacy. These include:

- Increasingly accurate biometric recognition systems that can identify individuals from images of the face or recordings of the voice
- De-anonymization techniques that can identify individuals by efficiently combining increasing large volumes of digital data
- Techniques such as model inversion and membership attacks, that infer the properties of data from the machine learning models trained on those data. For instance, a membership attack can reveal whether a facial recognition system was trained on a specific individual's face.
- The Internet of Things – in the next two decades, trillions of devices, ranging from appliances to clothing, will be connected to the internet. If data from these devices are not sufficiently secure, they're likely to be used to reveal the identities and patterns of life of users.
- Finally, and most speculatively, in the long run, quantum computers could be used to defeat many existing encryption methods. This is unlikely to happen in the next two decades; but given the time it takes to implement new encryption systems, NIST is currently evaluating systems that would be secure against quantum computers.

Those are technologies likely to erode some aspects of privacy. There are also many new technologies likely to enhance privacy. Most of these involve advances in encryption. These include:

- Homomorphic encryption, in which mathematical operations are performed on encrypted data. For example, Alice could own a database of health records that are encrypted, while allowing Bob to calculate the number of patients in those records who have the flu, without Alice's data ever being decrypted. IARPA has worked with DHS on a pilot project called SPAR to demonstrate that such methods are practical. Existing systems are inefficient, but for problems that involve only millions of records, these systems can be used today. Other advances in encryption include:
- Secure multi-party computation, in which Alice and Bob jointly perform a computation, such as tallying election results, while keeping their own datasets private.
- Functional encryption, in which Alice gives a key to Bob so that Bob can perform a computation on encrypted data, but Bob can only perform the computation that Alice has authorized.

- Verifiable computing, to prove to Alice that a computation Bob claimed to have done was done correctly.
- Zero-knowledge proofs, in which Alice proves to Bob that she knows a secret, such as a password, without having to give up that secret.
- Differential privacy, which adds controlled noise to data so that individual information cannot be extracted.
- Lastly, there are new AI methods that learn from encrypted data. Such methods would allow us to find patterns in large datasets, such as the causes of cancer from patterns in health records, without needing to decrypt those records. This problem is a focus of IARPA’s SAILS program.

Those are several emerging technologies likely to enhance privacy. If you take nothing else from my statement today I hope you’ll encourage more demonstration projects involving homomorphic encryption. Policymakers often have to make difficult tradeoffs between privacy and security; the value of homomorphic encryption is that it can enhance both privacy and security at the same time.

Thank you for your time and I look forward to answering any questions later.