DREXEL UNIVERSITY
Thomas R. Kline
School of Law

Hannah Bloch-Wehba
Assistant Professor of Law

TESTIMONY OF PROFESSOR HANNAH BLOCH-WEHBA
Before a hearing of the New Jersey Assembly
Science, Innovation and Technology Committee
February 3, 2020

Chairperson Zwicker, Vice-Chair Carter, and members of the Committee on Science, Innovation, and Technology:

My name is Hannah Bloch-Wehba. I am an assistant professor at Drexel University's Thomas R. Kline School of Law, and I have been researching law enforcement's use of new technology for over six years. My focus is on transparency and accountability mechanisms that can protect the public's right to know what their government is up to. I am appearing here in my personal capacity, and the views I express here do not reflect any views of Drexel University or of the Kline School of Law.

Thank you so much for giving me the opportunity to share my views about the legislation under consideration by the committee today, A1210. I appreciate that the Committee is considering how to ensure that the use of facial recognition technology by law enforcement is transparent and accountable to the public. Facial recognition can be an important tool for law enforcement to investigate and deter crime. But as this legislation recognizes, facial recognition's efficiency and utility does not mean that it ought to be kept a secret from the public.

I applaud the Committee for introducing this legislation and taking a stand against law enforcement secrecy. But while this legislation is an important first step to ensuring that police technology is subject to democratic oversight and legislative control, I urge the Committee to consider more significant steps, either in this legislation or in additional legislation, to ensure that the use of facial recognition technology is truly accountable.

Facial recognition poses a grave threat to our privacy as well as to our freedoms of expression, association and religion protected under the First Amendment. Imagine that a police surveillance camera mounted outside of a church captures footage of each and every churchgoer; armed with facial recognition, each of them could be identified with ease. Or imagine that undercover police use a facial recognition application to identify protesters at a demonstration. These and similar uses raise significant questions about our constitutional rights to associate freely and anonymously, and they raise the specter of a world in which any individual can be identified at the blink of an eye.

Unlike ordinary surveillance, individuals often never learn that they have been identified or tracked in this manner. And the public too seldom knows that the law enforcement agencies that are keeping them safe are using this technology in ways that we might not think are appropriate.

I commend the Committee for recognizing that we need much more vigorous public scrutiny and debate regarding police technologies. But this legislation does not go far enough to protect individual rights or to ensure that the public has the opportunity to weigh in on these fundamental changes in policing. Indeed, by taking such a modest step, the Committee risks sending the message that public hearings alone are sufficient to ensure that the public can weigh in on facial recognition technology.

First, I am concerned that the proposed legislation does not adequately address the risks of biometric surveillance. Facial recognition is only one type of biometric surveillance. Other systems, such as gait and voice recognition, pose equivalent threats to privacy and to expressive freedoms. By requiring public hearings for facial recognition, but not other biometric surveillance technologies, the legislation might actually incentivize law enforcement to deploy other, more advanced technologies that would not be addressed by this legislation.

Moreover, the way the legislation is drafted leaves me uncertain about whether it would capture voluntary cooperation with private-sector companies. For example, Amazon's home surveillance subsidiary, Ring, has entered into agreements with law enforcement to encourage consumers to adopt Ring products. Ring is also reportedly working on integrating facial recognition within the hardware. If these reports are true, then law enforcement will be able to seek footage from Ring or Ring users that may use facial recognition technology to identify individuals. Because the technology is in the hands of the private sector, law enforcement might not consider this to be covered by the language in the proposed legislation.

Second, while public hearings are an important way of fostering public input and debate, they are a limited one. Many individuals will find it difficult to participate in a one-time hearing, even one on such an important issue. Requiring a second hearing after five years, as the legislation under consideration does, recognizes the likelihood that the uses of facial recognition might change over time. But five years is a long time to wait for a second opportunity to weigh in, particularly so in light of the rapid pace of innovation and development in this field. In contrast, notice-and-comment rulemaking, for instance, provides the public with an opportunity to submit comments in writing over a specified period of time. It is my belief that notice-and-comment allows for a more engaged and meaningful dialogue between law enforcement and the public than holding a public hearing.

Other models are more effective at ensuring that the public knows exactly how the police are using new technologies. No affirmative legislation authorizes law enforcement to use facial recognition in this state, and no law restricts how it does so. Under current frameworks, law enforcement is not required to set standards for how they use facial recognition systems, and even if they do set standards, they might not be publicly available. The systems law enforcement uses are not subject to third-party oversight or auditing. They are often procured from vendors whose practices are obscure. And no law requires law enforcement agencies to notify defendants or other affected people that they have been identified using facial recognition.

Given facial recognition's widespread impact on individual rights and liberties, this Committee should take this opportunity to do more to ensure that the residents of New Jersey are empowered to make meaningful decisions about law enforcement surveillance. Law enforcement could—and should be required to—set standards for how they use facial recognition systems, and those standards ought to be publicly available. Law enforcement could—and should be required to—notify defendants whom it identifies using facial recognition technology. Law enforcement could—and should be required to—conduct impact assessments that consider how facial recognition technology affects expressive and privacy rights. And the systems that law enforcement relies upon could—and should—be subject to rigorous independent auditing, the results of which ought to be publicly available.

I commend the Committee's work on this important issue and thank you for the opportunity to testify and share my thoughts on this legislation.