CHHS

TESTIMONY IN SUPPORT OF SB0905 - CRIMINAL LAW – IDENTITY FRAUD – ARTIFICIAL INTELLIGENCE AND DEEPFAKE REPRESENTATIONS

JUDICIAL PROCEEDINGS

FEBRUARY 26, 2025

Chair Smith, Vice Chair Waldstreicher and Members of the Committee:

My name is Ben Yelin, and I am the Program Director for Public Policy & External Affairs at the University of Maryland Center for Health and Homeland Security. I am testifying on behalf of myself and Christopher Webster, the Center's Program Director for Cybersecurity and Emerging Technologies. Over the past few legislative sessions, our Center has worked closely with Senator Hester on legislation relating to artificial intelligence, cybersecurity and other matters. After the horrific incident at Pikesville High School, we began working with Senator Hester, Senator Hettleman, and other members of the General Assembly on a potential policy solution that would properly disincentivize the distribution of what we call Deceptive Deepfakes.

We were pleased to come before this committee to testify in favor of a similar bill SB362, which would impose criminal penalties on the distribution of forged digital likenesses. The bill was based on a theory that the harm caused by Deceptive Deepfakes was not just to individuals depicted, but to society writ large. Unregulated distribution of Deceptive Deepfakes would undermine our collective trust in testimonial evidence, just the way a forged document would undermine confidence in all other signed documents.

Members of this committee asked some important questions about SB362 and raised several legitimate concerns. First, the bill might be broad enough to criminalize even *de minimis* alterations of photos, audio or video. And second, legally cognizable harm to any individual was not a prerequisite, which could have opened the door for overbroad enforcement. There are some negative uses of Deceptive Deepfakes that would not be criminalized here, that would be in SB362. For example, a person could distribute a video of oneself rescuing people from a burning building and present it as genuine without facing criminal penalties. While we support the approach taken in SB362, we also acknowledge that a narrower approach, focused on Deceptive Deepfakes that cause specific harms to an individual, would achieve most of the policy goals that we identified in trying to address the incidents like the one in Pikesville.

SB905 would criminalize the knowing and willful creation and distribution of Deceptive Deepfakes with the intent to defraud, mislead or cause harm to another person. Harm is defined to not only include physical and emotional injury, but also economic damages. The bill also prohibits the knowing, willful and unconsented use of personal identifying information, including biometric data, to cause harm. The bill also would provide for a cause of action in civil court for a person harmed by any of the criminalized activity identified in the bill.

The prohibitions in this bill would certainly cover the most egregious uses of Deceptive Deepfakes: those that use a person's image or voice to create or distribute false audio or video in a way that would hurt a person's livelihood, economic standing or reputation. A tool like SB905 in the toolbox of any prosecutor, especially considering the significant penalties therein, would provide a proper disincentive for the type of crime we saw perpetrated at Pikesville High School. This approach would also ensure that *de minimis* changes to audio or video, or those that would not cause harm to any person, are legally protected.

For these reasons, we respectfully request a favorable report on SB905.