Yelin Testimony - SB905 2025 .pdf
Uploaded by: Ben Yelin
Position: FAV

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.

SB905_JPR_Morgan_FAV.pdf
Uploaded by: Karen Morgan
Position: FAV

AARP Maryland

One Park Place | Suite 475 | Annapolis, MD 21401-3475
1-866-542-8163 | Fax: 410-837-0269
aarp.org/md | md@aarp.org | twitter: @aarpmd
facebook.com/aarpmd

SB 905 – Criminal Law – Identity Fraud – Artificial Intelligence and Deepfake Representations
FAVORABLE
Senate Judicial Proceedings Committee
February 26, 2025

Good afternoon, Chairman Smith and Members of the Senate Judicial Proceedings Committee. My name is Karen Morgan, and I serve on the Executive Council for AARP Maryland. Representing nearly 850,000 members, AARP Maryland is one of the largest membership-based organizations in the state. We thank Senator Hester for sponsoring this important legislation.

AARP is a nonpartisan, nonprofit organization dedicated to empowering people to live their best lives. We advocate on key issues affecting families, including health care, financial security, retirement planning, and protection from financial abuse.

SB 905 would specifically criminalize the intentional, unauthorized use of artificial intelligence (AI) and deepfake representations to cause financial or other harms. The bill would make a convicted perpetrator subject to maximum prison sentences of 5 to 10 years and/or maximum fines of $10,000 to $15,000, depending on the number of victims harmed. It would allow victims to bring civil suit against the criminals who commit these acts. In the courts, the bill also authorizes the imposition of injunctive or other appropriate relief.

AARP Maryland supports SB 905 because, quite simply, Maryland citizens need help. We are inundated with reports of data breaches, spam emails, spam texts, and spam phone calls. We know that just trying to communicate with family friends – especially through social media, could make us subject to the harvesting and weaponization of our images as well as our personal information. Data brokers are legally authorized to scrape all kinds of personal information – even Social Security numbers – and bundle them for sale to anyone who wants to buy them.

As consumers, we have very little control over the collection of our images and information. But if someone decides to use that information to cause financial or other harm, at least that criminal would be subject to significant criminal penalties under this bill. SB 905 is important because it anticipates the use of technology to steal money.

We are all familiar with the "grandparent scam" where a crook contacts a person and tells them that their grandchild is in desperate trouble and the only way to help them is to immediately "send money". We've heard enough about this scam to be skeptical about a strange voice on the phone. But what if the voice is an exact replica of the grandchild's voice? What if a video is created that portrays the grandchild in serious trouble – being carted off in handcuffs under police escort, for example? While the extent to which these kinds of deepfakes are happening is unclear at this time,

we know that they can happen. Maryland citizens are an enticing target for identity theft criminals. In 2023, Maryland ranked 11th in the nation for reported identity fraud incidents, according to the Federal Trade Commission. AARP research indicates that reported incidents are only a fraction of all the identity theft crimes that occur because people are reluctant to report when they are victimized by these criminals.

Given the widespread use of AI and deepfake representations, we believe that designation of this new crime as a felony is appropriate. It is also appropriate to make these criminals subject to civil suit so that victims can take some action to at least try to recover what has been wrongfully taken from them. These types of crimes strike at the core of everything we value and hold dear. The response of the criminal justice system should reflect the impact of these types of crimes.

Frankly, we need more tools against perpetrators who use AI to scam or fraud Marylanders. SB 905 provides additional enforcement remedies. AARP believes **that policy makers should provide privacy protections while enabling meaningful innovation and data-driven decision-making**—data privacy and security laws and regulations should provide meaningful data privacy and security consumer protections. In addition. AARP believes it is:

- **Imperative to safeguard consumer choice and control**—consumers should control the extent to which their personal information may be collected, analyzed, shared, and sold.
- **Ensure heightened protections for sensitive data**—data that are sensitive and pose significant risk to the consumer if disclosed should receive heightened privacy and security protections.
- **Promote privacy and security by design**—privacy and security protections should be embedded into products and services.
- **Foster transparency**—organizations should provide accurate and understandable information to consumers about their privacy and security practices.
- **Ensure accountability**—privacy and security laws and regulations should include robust enforcement mechanisms to ensure compliance.

AARP Maryland respectfully requests that the Senate Judicial Proceedings Committee issue **a favorable report on SB 905**. For any questions, please contact Tammy Bresnahan, Director of Advocacy for AARP Maryland, at tbresnahan@aarp.org or **410-302-8451**.

SB905- AI Identity Fraud Testimony Draft.docx.pdf
Uploaded by: Katie Fry Hester
Position: FAV

KATIE FRY HESTER
Legislative District 9
Howard and Montgomery Counties

Education, Energy, and
Environment Committee

Chair, Joint Committee on
Cybersecurity, Information Technology
and Biotechnology

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

Annapolis Office
James Senate Office Building
11 Bladen Street, Room 304
Annapolis, Maryland 21401
410-841-3671 · 301-858-3671
800-492-7122 *Ext.* 3671
KatieFry.Hester@senate.state.md.us

Testimony in Support of SB 905 - Criminal Law – Identity Fraud – Artificial Intelligence and Deepfake Representations

February 26, 2025

Chair Smith, Vice-Chair Waldstreicher, and members of the Judicial Proceedings Committee:

Thank you for your consideration of Senate Bill 905, *Criminal Law – Identity Fraud – Artificial Intelligence and Deepfake Representations*. This legislation is essential in strengthening Maryland's ability to combat identity fraud by addressing the evolving threats posed by artificial intelligence (AI) and deepfake technology.

The rapid advancement of AI technology has made it easier than ever to create highly realistic synthetic media: including altered images, videos, and audio recordings. While these tools have legitimate applications, they also present serious risks when misused for fraud, harassment, or deception. The malicious use of AI-generated content to impersonate individuals threatens personal privacy, financial security, and public trust in digital systems. The consequences of this misuse include:

- Financial harm- Victims suffer economic losses from fraudulent unauthorized transactions and identity fraud. This is made much easier with AI being used to fake someone's voice for voice identification purposes.
- Criminal activity- AI-generated content can help criminal enterprises create counterfeit identification documents, including fake driver's licenses and fraudulent credentials for law enforcement, government, and banking institutions.[1]
- Emotional and psychological distress- Individuals experience severe personal and reputational harm due to manipulated content.
- Erosion of trust- The integrity of digital communication and online systems is undermined.
- Exploitation and manipulation- Bad actors use AI to impersonate individuals for personal gain.

[1] https://www.ic3.gov/PSA/2024/PSA241203#:~:text=Identifying%20information%20about%20the%20individuals,%E2%86%A9

Earlier last year, a troubling incident at Pikesville High School highlighted the urgency and threat of this issue. The school's athletic director used deepfake technology to create a false audio recording of the school's principal, leading the public to believe he had made racist and antisemitic remarks. This falsified audio, while not technically advanced, required only a basic recording of the principal's voice and a $ 5-a-month AI tool.[2] The incident served as an important warning and call to action: anyone with minimal resources can now use AI to commit identity fraud.

Other states are already taking action. Last year, New Jersey introduced bipartisan legislation extending identity theft laws to include fraudulent impersonation through AI and deepfake technology.[3] Maryland must take similar steps to protect its residents from this growing threat.

Ultimately, presenting a false representation of someone utilizing AI is a form of identity theft. SB 905 ensures that Marylanders are safeguarded against AI-driven identity fraud by:

1) **Expanding Definitions**
    - **a)** Updating the legal definition of "personal identifying information" to include biometric data and digital signatures.
    - **b)** Incorporating legal definitions for AI, deepfake technology, and false personation records, covering any AI-generated media used to impersonate individuals.
2) **Providing Civil Restitution and Victim Support:**
    - **a)** Empowering courts to order civil damages for victims, including reimbursement for clearing credit histories and resolving fraudulent debts.
3) **Prohibiting Misuse of Personal Information:**
    - **a)** Criminalizing the unauthorized acquisition, use, or sale of personal identifying information for fraudulent purposes.
    - **b)** Prohibiting the creation and distribution of deepfake or synthetic media that impersonate individuals without consent and causes harm.
4) **Strengthening Penalties:**
    - **a)** Establishing penalties based on the value of benefits obtained from the crime or the harm caused to the victim(s).
    - **b)** Imposing stricter consequences for violations involving multiple victims, election interference, or harm to minors.
5) **Enhancing Enforcement:**
    - **a)** Granting law enforcement broader authority to investigate and prosecute identity fraud cases across jurisdictions.

---

[2]https://www.thebaltimorebanner.com/education/k-12-schools/pikesville-principal-ai-GXGDPO5W6JHFBGES25SYQ2KM5M/

[3] https://pub.njleg.gov/Bills/2024/A4000/3912_I1.HTM

b) Establishing clear guidelines for interagency coordination and reporting to ensure effective enforcement.

Maryland must act now to address the dangers posed by AI-driven identity fraud. SB 905 provides the necessary legal tools to combat these emerging threats and to safeguard our communities.

Thank you for your consideration, I urge a favorable report of SB0905.

Sincerely,

Senator Katie Fry Hester
Howard and Montgomery Counties

OSPSupportSB905.final.pdf
Uploaded by: Sarah David
Position: FAV

CHARLTON T. HOWARD III
State Prosecutor
SARAH R. DAVID
Deputy State Prosecutor
ABIGAIL E. TICSE - MARY W. SETZER
JOYCE K. McDONALD - BRITTANY DUNKLOW
Senior Assistant State Prosecutors
STEPHANIE HADDAD
Assistant State Prosecutor

STATE OF MARYLAND

OFFICE OF
THE STATE PROSECUTOR

40 W. Chesapeake Avenue
Suite 300
Towson, MD 21204
Telephone (410) 321-4067
1 (800) 695-4058
Fax (410) 321-3851

SUPPORT FOR SB 905

Mr. Chairman and Members of the Judicial Proceedings Committee Committee:

We are writing to express the support of the Office of the State Prosecutor for Senate Bill 905. The Office of the State Prosecutor is tasked with enforcing political corruption and police misconduct cases throughout Maryland and believes that this legislation will help address the challenges artificial intelligence presents to the integrity of the electoral process as well as ensuring that people's identity is not manipulated using technology to defraud the public.

The Office of the State Prosecutor

The Office of the State Prosecutor is an independent agency within the Executive Branch of government. The Office is tasked with ensuring the honesty and integrity of State government and elections by conducting thorough, independent investigations and, when appropriate, prosecutions of criminal conduct affecting the integrity of our State and local government institutions, officials, employees, and elections.

SB 905- Criminalizing the use of artificial intelligence

SB 905 alters Maryland's existing identity theft statute to include the use of artificial intelligence and deep fake technology. This uses the same theory of identity theft with the criteria being that this technology is indistinguishable from an identifiable human being and that it was crafted with that intent. It is important to note that the requirement is that the person has to have fraudulent intent, there is no consent from the person, and there is intent to cause harm.

The crime is a felony not only due to the serious adverse ramifications using artificial technology causes but also because of the time and resources required for law enforcement to investigate the source of the technology. Discovering who committed the act often takes more than a year by the time the data is analyzed (especially if it is not known who created the deepfake). It is also a way to manipulate public information in a way that can impact people's lives, especially the lives of young people, in a very negative way. Cases in Maryland have included faking the voice of a high school principal to make the community believe he made antisemitic and racist remarks and a person manipulating images to look like minors were engaged in sexual activity and sharing it within their school community. These cases are extremely difficult to prosecute under our current laws.

This law is drafted to truly criminalize the identity theft component. The requisite criminal intent would not be met by something satirical or meant to entertain. Rather, by encapsulating

this language in the identity theft statute, it makes it clear that it is not criminalizing the fact the material is artificial, but the intent to make people believe it is not.

We encourage a favorable report on SB 905.

Sincerely,

CHARLTON T. HOWARD, III
STATE PROSECUTOR

SB 905 - Criminal Law - Identity Fraud - Artificia
Uploaded by: Scott Shellenberger
Position: FAV

Bill Number: SB 905
Scott D. Shellenberger, State's Attorney for Baltimore County
Support

WRITTEN TESTIMONY OF SCOTT D. SHELLENBERGER,
STATE'S ATTORNEY FOR BALTIMORE COUNTY,
IN SUPPORT OF SENATE BILL 905
ARTIFICIAL INTELLIGENCE AND DEEPFAKE REPRESENTATIONS

I write in support of Senate Bill 905 which fills a large gap in this day and age of committing crimes using computers and more specifically Artificial Intelligence.

What if you are a County Executive, a Police Chief or a State Senator and there is someone out there who has a grudge against you. Nowadays they can get revenge by using Artificial Intelligence to take prior statements or videos you have made that have been recorded and turn that into anti-racial or anti-anything and make those statements very public. What if that audio/video is released to the public and causes regular people to get angry and upset at you. What if people are so upset that you need police protection. Right now in Maryland we do not have a statutory crime to charge that person. There is a hole in the Law that needs to be filled to make the crimes of today and the way they can be committed punishable. We need SB 905 to fill a gap in the Law.

The scenario I just outlined is not a made up story, it really happened. As you know Baltimore County has such a case and because it is a pending trial I will not talk about the facts or details of that case. When that incident happened I picked up this book, Criminal Laws, and searched and searched and found nothing directly on point to what they did. While I like Senate Bill 362 for its simplicity perhaps we need more maybe both.

Senate Bill 905 fills that gap by making it a crime to use Forged Digital Likeness to misrepresent and likely to deceive. Senate Bill 905 uses the word Forged Digital Likeness that is defined as a visual representation of a person or audio recording of an identifiable person's voice. That's the one we needed in the Pikesville case. Under the new Law we must prove that it was created to imitate how the person looks or sounds. The key is the state must prove that it is likely to deceive a reasonable person. That would provide the needed Law if it ever happens to a County Executive of Police Chief or a Senator.

Senate Bill 905 expands on this by not just outlawing the use of visual or audio imitation but expands upon those by adding photographs, a film, video, digital image, a picture or computer generated image, etc. Senate Bill 905 is trying to out law what criminals are likely to develop in the years to come.

I envision an age when a grandparent may get an urgent Facetime with who the grandparent believes is their grandchild. AI may become so advanced that this audio

and visual encounter may seem so real that the fake grandchild receives money that they requested. We have to try to stay ahead of what criminals are about to embark upon.

Senate Bill 905 is a much needed Bill in this day and age of how crimes can be committed.

I urge a favorable report.

Legislative Letter SB0905_Burns.pdf
Uploaded by: Brooke Burns
Position: FWA

February 24, 2025

Dear Honorable Senators,

My name is Brooke Burns and I am currently an 18-year-old student at Linganore High School in Frederick, MD. I am submitting this letter to register strong support for **SB0905-Crimial Law – Identity Fraud – Artificial Intelligence and Deepfake Representations** with amendments. This legislation will provide sorely needed additional protection, however, it only covers actions knowingly, willfully, and with fraudulent intent. It **does not include reckless disregard that the artificial intelligence and deepfake representations will be used to harm victims**.

This legislation would not provide protection to me in a situation I recently encountered where a **male classmate of mine created graphic sexually explicit social media accounts impersonating me and many other high school girls (all minors)**. He used pictures of us along with nude pictures of unknown women with the intent of implying that it was us. He confessed to the Frederick County police that he created these pornographic social media accounts, as well as, emails, etc. using the names/likeness of the girls. **Incredibly, the Maryland State's Attorney said that what he did does not constitute a crime under the current laws of Maryland!**

The best the State's Attorney could do was to attempt to charge him for identity theft, however, after being challenged by the perpetrator's attorney, she had to withdraw those charges. She stated that the current laws of Maryland require someone who is charged with identity theft to have received financial benefit from the identity theft. Unfortunately, the State's Attorney did not identify a financial benefit to the perpetrator. She said that federal law allows for non-monetary benefit in charging for identity theft but not Maryland law.

What this person did would not be covered under the current proposal for SB0905 because he didn't do this with the <u>intent</u> to harm me or the other girls. However, he should have known what he did would likely cause harm to us because these false images were out on the web for anyone to find. Without adding a reckless disregard component to SB0905, he could not be held accountable under SB0905 while me and the other girls would have images representing us on the web that could severely harm us in our future. In addition, we are left to cover the costs to attempt to remove these false images of us online and not the perpetrator!

Maryland enacted Grace's Law in October 2023. This law prohibits a person from using electronic communication that alarms or seriously annoys someone 1) with the intent to harass, alarm or annoy the other person, 2) after receiving a reasonable warning or request to stop and 3) without a legal purpose. However, in our case, the State's Attorney indicated that she could not find evidence that these accounts were set up with the intent to harass, alarm or annoy the girls. Therefore, Grace's Law does not apply to the atrocious acts the perpetrator committed in our case. Per the Frederick County detective, the perpetrator admitted to setting up these social media accounts in order to pose as underage girls to attempt to get adult males to contact him for his sexual gratification.

I and the other girls have explicit sexual social medial accounts bearing our name and pictures that we had no part in creating. Furthermore, these accounts may never be fully erased from our online presence. This could have a significant impact on us in the future when applying for colleges, employment opportunities, etc. if someone finds this information online. It is outlandish that we have to suffer all of this while the perpetrator cannot currently be charged for any crimes in Maryland related to the things he did to us!

Below is a more detailed discussion of the events and impact the perpetrator's actions have had on me and the other girls. I am hoping that after you read this, you will get a better feel for the extent of his actions.

When this all started for me, I was a 16 – year old high school student living in Frederick County, MD. I am a victim of cybercrime that has profoundly impacted my psychological well-being, social life, and academic performance. It has also created an explicit and pornographic digital footprint that is virtually impossible to eliminate. I am shocked that our current laws did not protect me.

On December 5, 2023, Frederick City Detectives from the Cyber Crime Unit came to my house because they received a tip from the National Center of Missing and Exploited Children that a sexually explicit account on X (Twitter) was created that contained pornographic (nude) pictures of me. At the time, the detectives indicated that one of my friends also had a similar online profile on X. Subsequent to that date, a total of seven people had sites created by the perpetrator (six minors and one male adult). In total, seventeen minor girls had pictures included on these social media sites created by the perpetrator.

The trauma started that night. I was terrified, angry, and scared for my physical safety. At that time, the fear around the unknown of who did this, why and if it was a person that was stalking me and may come to our house was all consuming. I asked my dad to double-check to make sure all the doors were locked and the alarm was set and I was afraid to sleep alone in my own bedroom.

A few days later, the Frederick County sheriff's department identified that the IP address for the fake X account belonged to a student who is in my second period class. We started scouring the internet and found many accounts and more victims, many of which are my close friends. To date fifteen accounts have been identified to impersonate me and over eighty accounts and counting for all the victims related to the case. It is difficult to explain the graphic nature and the egregiousness of these sites. These sites contain explicit content, specifically marketing me and others as underage. The sites show my picture and engage with users to respond to sexually explicit questions.

Some of the sites entice followers to interact with us including asking for them to email to get nude pictures. The accounts and postings have lewd and suggestive comments posted by hundreds of unknown online users. The sites have links to other accounts that say things like – "to see my dirty little secrets click here". And this is benign to many of the statements. One site of a victim had 750,000 views and was averaging 99,000 more views per month.

My parents worked with the Frederick County School Board and the perpetrator was removed from my school. Even with him out of my school, this crime destroyed my sense of security. They have

caused me to miss school and change my social behavior. I did not want to interact with him in the community and am afraid that he will continue to create false and harmful content about me.

I do not fully know how this will follow me throughout my life. I have even had someone who viewed the fraudulent sites reach out to me on my personal account. This is terrifying! Will more users participating in these fraudulent sites reach out to me? Will colleges or future employers look at this online presence and make adverse decisions about me?

I did nothing wrong! I did not take or post any inappropriate pictures of myself. The impact of this perpetuator's actions has been devastating to my family. In addition to the emotional trauma caused, my parents have also had to spend a significant amount of time and money to try to identify and attempt to take down as many fraudulent accounts as possible. To date, only a few of the sites have been taken down. They knew we would be unable to find all the fraudulent accounts so they hired a cyber forensics company to scrub the internet and locate as many sites as they could. The cyber forensics expert told us that the number of sites is egregious and that they think it would be naïve to expect that they will be able to identify and erase all the digital footprint. This **will** continue to follow me as the digital footprint is impossible to get rid of.

My parents expect to continue to incur significant legal fees to help force the online providers to close these accounts, to continue to work with the forensics company to identify the sites – as their expert opinion is that more work will be needed over the upcoming years especially to identify and close fraudulent accounts.

My parents and I are sickened that the laws do not adequately address the damage to my life and our lives.

As mentioned above, we have worked with the State's Attorney's Office and this perpetrator was not found guilty of breaking a law for his actions in this case. How is this possible? Someone for their own personal gain – created false accounts, impersonated me online with sexually explicit pictures, for the purpose of engaging with men that wanted to interact with minor girls.

In conclusion, I am requesting that you support the passing of SB0905 with amendments to also include a component for the reckless disregard for the risk that the artificial intelligence and deepfake representations would harm the victims.

I would like to take this devastating situation and know that I made a difference in helping to protect other teenagers from similar experiences.

I would appreciate the opportunity to answer your questions. My parent's email is abnburns@comcast.net and Ann Burns (my mom's) cell number is 410-707-3022.

Thank you for your time and consideration.

Sincerely,

Brooke E. Burns

Brooke Burns

[MD] SB 905_deepfakes_TechNet.pdf
Uploaded by: margaret durkin
Position: FWA

TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

TechNet Mid-Atlantic | Telephone 717.585.8622
www.technet.org | @TechNetMidAtla1

February 24, 2025

The Honorable William Smith
Chair
Senate Judicial Proceedings Committee
Maryland Senate
2 East Miller Senate Office Building
11 Bladen Street, Annapolis, MD 21401

RE: SB 905 (Hester) - Criminal Law – Identity Fraud – Artificial Intelligence and Deepfake Representations - Favorable with Amendments

Dear Chair Smith and Members of the Committee,

On behalf of TechNet, I'm writing to share our comments on SB 905 related to artificial intelligence and deepfake representations.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents over 4.5 million employees and countless customers in the fields of information technology, artificial intelligence, e-commerce, the sharing and gig economies, advanced energy, transportation, cybersecurity, venture capital, and finance. TechNet has offices in Austin, Boston, Chicago, Denver, Harrisburg, Olympia, Sacramento, Silicon Valley, Tallahassee, and Washington, D.C.

Artificial intelligence has the potential to help us solve the greatest challenges of our time. It is being used to predict severe weather more accurately, protect critical infrastructure, defend against cyber threats, and accelerate the development of new medical treatments, including life-saving vaccines and ways to detect earlier signs of cancer. However, recognizing and addressing the genuine risks associated with AI is crucial for its responsible advancement.

In the context of regulating AI in deepfakes, liability should be solely on the natural person who is the bad actor violating the law. Further, we believe that any state law should align with federal exemptions contained in Section 230 of the federal code. As such, we're requesting the following language be added to SB 905:

TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

- **"As such terms are defined in 47 U.S.C. § 230, an interactive computer service is not liable for content provided by another person in violation of this act."**

Thank you for the opportunity to share our comments on SB 905 and please don't hesitate to reach out with any questions.

Sincerely,

Margaret Durkin

Margaret Durkin
TechNet Executive Director, Pennsylvania & the Mid-Atlantic

MD S.B. 905 memo in opposition.pdf
Uploaded by: David Horowitz
Position: UNF

THE MEDIA COALITION
DEFENDING THE FIRST AMENDMENT SINCE 1973

American Booksellers Association Association of American Publishers Authors Guild Comic Book Legal Defense Fund
Entertainment Software Association Freedom to Read Foundation Motion Picture Association of America

Memo in Opposition to Maryland S.B. 905

The Media Coalition is concerned that S.B. 905 allows a civil cause of action that will inevitably have a chilling effect on speakers because it can be used by those with deep pockets to impose a financial punishment on publishers merely by suing even if they are unlikely to prevail. In addition, the cause of action allows a judge to impose an injunction to prevent publication. This is a prior restraint, which is almost always unconstitutional. We are also concerned about the lack of adequate definitions for key terms could make the legislation unconstitutionally vague and will also have a chilling effect on producers and distributors of media.[1]

The bill amends the existing criminal identity fraud statute to create a crime and a civil cause of action of using a "deepfake representation" with "fraudulent intent" to "mislead." "Deepfake representation" is defined as a photographic image or video that an ordinary person would believe is an actual, identifiable person. The image itself does not have to portray the person falsely to be a "deepfake" under the bill. The terms "fraudulent intent" and "mislead" are not defined in the bill.

A violation of this section is subject to up to 5 years in prison, a fine of $10,000, or both. In addition, the bill—unlike all of the other identity fraud crimes in this section—creates a civil cause of action to allow a private suit against a person who uses a deepfake. A prevailing plaintiff is entitled to damages and injunctive relief, including an *injunction prior to publication* of the image.

The civil cause of action could lead to a publisher or distributor of a deepfake being sued for publishing (or intending to publish) an image that is intended to be deeply critical of the person depicted, if the publication would be "misleading" and potentially "misrepresent[s]" that person, even if the conduct would not be criminally fraudulent. There is a long tradition of parody, satire, commentary and other speech about matters of public interest or debate using hyperbole, exaggeration and sarcasm to criticize or condemn the powerful or wealthy.[2] In a world where

[1] Media Coalition Inc., is a trade association that engages in legislative and legal advocacy to defend the First Amendment right to create, produce and distribute books, films, home video and video games. The trade associations and organizations that comprise Media Coalition have many members throughout the country, including Maryland: authors, publishers, booksellers and librarians, producers and retailers of films, home video and video games.

[2] Notably, the First Amendment provides especially strong protections to works that constitute parody, satire, and other matters of public concern—as these are considered "core speech" worthy of protection even if it is false and misleading. In *Alvarez*, even the Justices who would have upheld a law criminalizing lying about receiving a military honor cautioned that speech about matters of public concern would still be protected. In his dissent, Justice Alito wrote: "[A]ny attempt by the state to penalize purportedly false speech would present a grave and unacceptable danger of suppressing truthful speech. Laws restricting false statements about philosophy, religion, history, the social sciences, the arts, and other matters of public concern would present such a threat." *U.S. v. Alvarez*, 567 U.S. 709, 751 (2012). See also *Hustler Magazine v. Falwell*, 485 U.S. 46 (1988)

many people dispute what is the truth, a statute which potentially creates liability for "misleading" conduct makes the media vulnerable to being punished for publishing work that is protected by the First Amendment. S.B. 905 will cause publishers and distributers to fear that a wealthy or powerful person—unhappy that a critical, satirized representation of them being published—will bring a lawsuit to obtain an injunction against First Amendment protected speech on claims that a digitally-altered image was misleading, and imputing to the publisher a malicious intent for the distribution (or anticipated distribution) of the image. Even if a publisher prevails, a suit would cost a substantial amount of money and time. It is an increasingly common practice of those with great wealth to sue the media not to prevail but to impose a financial cost (and block, even temporarily, the publication of unflattering portrayals). Frequently, the mere threat of costly and prolonged litigation can prompt self-censorship by producers and distributors—which is an unconstitutional chilling effect. See *Baggett v. Bullitt*, 370 U.S. 360 (1964).

The potential problems raised by the civil cause of action are compounded because S.B. 905 permits a "preventative" injunction as a remedy to the civil cause of action. This is a prior restraint to speech, which is "the most serious and least tolerable infringement on First Amendment rights," and faces a "heavy presumption against its constitutional validity." *Neb. Press Ass'n v. Stuart*, 427 U.S. 539, 558-59 (1976) (citation omitted). As the Supreme Court explained in *Alexander v. U.S.*, "[t]he term 'prior restraint' is used 'to describe administrative and judicial orders *forbidding* certain communications when issued in advance of the time that such communications are to occur.' Temporary restraining orders and permanent injunctions — *i.e.*, court orders that actually forbid speech activities — are classic examples of prior restraints." 509 U.S. 544, 550 (1993) (internal citations omitted) (emphasis added). As such, the legislature must carefully limit the courts authority to impose an injunction to speech that is illegal and, therefore, outside the protection of the First Amendment. Misleading speech, even if communicated with a malicious intent may not qualify.

The lack of clear definitions in S.B. 905 adds to publishers' fears about being sued and it raises potential constitutional vagueness concerns. The lack of stringent definitions gives potential plaintiffs greater latitude in filing lawsuits seeking to financially punish or silence speakers rather than prevailing in the suit. On the one hand, S.B. 905 could be read to require genuinely criminal intent to establish liability (for either a criminal or civil cause of action). However, that is not clear from the text of the bill. The term "mislead" is not defined in the bill, but the common definition of the term is "to deceive or lead astray." This is not an inherently criminal act, and many instances of "misleading" speech are constitutionally protected.[3] Also, the term "fraudulent intent" could be substantially more expansive and therefore impose liability for non-criminal (and constitutionally protected) speech. "Fraudulent" is not defined in the statute, and its ordinary meaning includes acts of "deceiving or mispresenting" something—and a common synonym for the term is "dishonest." Neither "deceitful" nor "dishonest" speech is inherently illegal, and could include speech such as parodies and satire that are constitutionally protected.

[3] As a core First Amendment principle, false speech is protected as long as it was not communicated to gain a tangible benefit. *U.S. v. Alvarez*, 567 U.S. 709 (2012) ("The remedy for speech that is false is speech that is true. This is the ordinary course in a free society."). In *Alvarez*, the U.S. Supreme Court held that an attempt to ban or regulate false or misleading speech is impermissible unless it is linked to a specific, tangible harm or a malicious intent to cause such a harm.

Speech which is so vague so to "permit within the scope of its language the punishment of incidents fairly within the protection of the guarantee of free speech is void, on its face, as contrary to the Fourteenth Amendment." *Winters v. New York*, 333 U.S. 507, 509 (1948). This doctrine mandating clear restrictions is critical to provide certainty to publishers, to avoid those enforcing speech restrictions from acting "in an arbitrary or discriminatory way," and "to ensure that ambiguity does not chill protected speech." *FCC v. Fox TV Stations, Inc.*, 567 U.S. 239, 253-54 (2012) (internal citation omitted).[4]

In light of these concerns, we respectfully ask you to protect the First Amendment rights of all the people of Maryland and amend or defeat S.B. 905. We would welcome the opportunity to work with the legislature to address these issues. If you would like to do so, please contact me at 212-587-4025 or by email at horowitz@mediacoalition.org.

[4] *See also Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 871–72 (1997) ("The vagueness of such a regulation raises special First Amendment concerns because of its obvious chilling effect on free speech."); *Vill. of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 499 (1982); *Keyishian v. Bd. of Regents*, 385 U.S. 589, 604 (1967) (quoting *NAACP v. Button*, 371 U.S. 415, 432-33 (1963)) ("'Because First Amendment freedoms need breathing space to survive, government may regulate in the area only with narrow specificity.'").

MPA Maryland SB 905 Memorandum in Opposition.pdf
Uploaded by: Renata Colbert
Position: UNF

MOTION PICTURE ASSOCIATION

SB 905 / HB 1425
Memorandum of Opposition
February 24, 2025

The Motion Picture Association, Inc. ("MPA") respectfully opposes SB 905/HB 1425 (the "Bill") and offers proposed changes to the Bill as described herein.[1]

The MPA's members use computer-generated imagery for a wide array of purposes. They recreate historical events. They modify images, video, and audio to enhance news reports, aid viewers and listeners in understanding content, create interesting visual effects, and age and "de-age" actors. Moreover, some MPA members create satire, parody, and comedy and use altered images and audio for this purpose. It is well-established that the First Amendment protects these expressions. *See, e.g., New York Times v. Sullivan*, 376 U.S. 254 (1964); *Hustler Magazine, Inc. v. Falwell*, 485 U.S. 46 (1988).

While the MPA appreciates that there are harmful uses of "deepfake" technologies, which may be appropriately constrained through criminal statutes, efforts to regulate the use of such technologies must be crafted to avoid chilling protected and valuable creative speech and legitimate news coverage. However, the current draft of the Bill does not offer such protections. Instead, the Bill opens the door for private individuals—including public figures who may be the subject of a digitally altered rendering—to bring claims against media companies to stop them from publishing content that the individual claims will be "misleading." For instance, a public figure who learns that they are the subject of a parodic "deepfake" in a movie or TV show, or the subject of a documentary that will use deepfake technology for certain representations within the film, could file a lawsuit to prevent the media from ever being released. This lawsuit may be without merit—as such representations are protected speech, and there may be no "fraudulent intent" in the decision to release the film or TV show—but that may not stop a motivated party from bringing litigation. Without a prosecutor acting as gatekeeper, the individual could rush to court with conclusory allegations of fraudulent intent, even where none exists. This would force a studio or broadcaster to engage in a costly legal battle to protect their First Amendment rights. By permitting such lawsuits to be brought even *before* the media is released, the Bill paves the way for courts to exercise a prior restraint on speech, which is particularly disfavored under the First Amendment. This also imposes substantial practical costs by disrupting carefully crafted release schedules, marketing plans, and promotional efforts.

[1] The MPA is a not-for-profit trade association founded in 1922 to address issues of concern to the motion picture industry. Since that time, MPA has advanced the business and art of storytelling, protecting the creative and artistic freedoms of storytellers, and bringing entertainment and inspiration to audiences worldwide. The MPA's member companies are: Netflix Studios, LLC; Paramount Pictures Corporation; Prime Amazon MGM Studios; Sony Pictures Entertainment Inc.; Universal City Studios LLC; Walt Disney Studios Motion Pictures; and Warner Bros. Entertainment, Inc. In addition, several of the MPA's members have as corporate affiliates major news organizations (including ABC, NBC, and CBS News, and CNN) and dozens of owned-and-operated local television stations with broadcast news operations.

With no express protections for parody, satire, news reporting, and other protected speech, the Bill may force MPA's members and others to choose between foregoing such digitally altered representations altogether and defending against costly but meritless lawsuits.

To prevent this chilling effect, the MPA proposes a carveout that expressly exempts the kinds of speech that the First Amendment protects. *See Schad v. Borough of Mt. Ephraim*, 452 U.S. 61, 65 (1981) ("Entertainment, as well as political and ideological speech, is protected; motion pictures, programs broadcast by radio and television, and live entertainment, such as musical and dramatic works fall within the First Amendment guarantee.").

The MPA proposes the following addition to the Bill as section (F)(3):

(3) IT IS NOT A VIOLATION OF SUBSECTION (F)(2) OF THIS SECTION TO CREATE, USE, OR OTHERWISE DISTRIBUTE ANY AUDIO OR VISUAL CONTENT, REGARDLESS OF WHETHER IT IS COMPUTER-GENERATED, THAT RELATES TO A MATTER OF PUBLIC INTEREST, OR THAT IS PARODY, SATIRE, COMMENTARY OR CRITICISM, OR WHICH INVOLVES WORKS OF POLITICAL OR NEWSWORTHY VALUE.

Notably, this exemption would bring the Bill's First Amendment protections in line with statutes passed in other states regulating deepfakes. *See, e.g.*, N.H. Rev. Stat. § 638:26-a(IV);[2] LSA-R.S. 14:73.13(C)(1).[3]

In addition, the MPA proposes to remove the private right of action in the Bill, striking the new proposed section (H). This will remove a substantial threat of frivolous litigation from individuals who may object to critical news coverage or satirized or parodic representations of them in the media, even if the digital representations at issue are not criminally fraudulent. Removing this provision will provide studios and broadcasters with the necessary assurances that

[2] "This section shall not apply to any of the following:
(a) An interactive computer service as defined in 47 U.S.C. section 230 for content provided by another party.
(b) Any radio or television broadcasting station or network, newspaper, magazine, cable or satellite radio or television operator, programmer, or producer, Internet website or online platform, or other periodical that publishes, distributes or broadcasts a deepfake prohibited by paragraph II as part of a bona fide news report, newscast, news story, news documentary or similar undertaking in which the deepfake is a subject of the report and in which publication, distribution, or broadcast there is contained a clear acknowledgment that there are questions about the authenticity of the materials which are the subject of the report.
(c) Any radio or television broadcasting station or network, newspaper, magazine, cable or satellite television operator, Internet website or online platform, or other periodical when such entity is paid to publish, distribute or broadcast an election communication including a deepfake prohibited by paragraph II, provided that the entity does not remove or modify any disclaimer provided by the creator or sponsor of the election communication.
(d) A video, audio or any other media that constitutes satire or parody or the production of which is substantially dependent on the ability of one or more individuals to physically or verbally impersonate another person without reliance on artificial intelligence."

[3] "'Deepfake' does not include any material that constitutes a work of political, public interest, or newsworthy value, including commentary, criticism, satire, or parody, or that includes content, context, or a clear disclosure visible throughout the duration of the recording that would cause a reasonable person to understand that the audio or visual media is not a record of a real event."

they will not be subject to bad-faith lawsuits and can continue to publish protected speech without fear of being brought into court.

The MPA welcomes the opportunity to answer questions and provide additional input on the Bill. Legislators and staff seeking further information may contact the MPA's consultants in Annapolis, Nick Manis and John Favazza, at nmanis@maniscanning.com and jfavazza@maniscanning.com.

Sincerely,

Renata

Renata Colbert
Senior Manager
State Government Affairs