Assembly Standing Committee on Consumer Affairs and Protection
Assembly Standing Committee on Science and Technology

September 20, 2024 Public Hearing

SUBJECT: Ensuring consumer protection & safety relating to the use of artificial intelligence

PURPOSE: Examining regulatory and legislative options to ensure consumer and public protection relating to the use of artificial intelligence.

The increasing integration of artificial intelligence (AI) in business, commerce, and retail settings has simultaneously increased concerns related to the rights of consumers and raised questions as to what form or level of regulatory protections maybe be appropriate or feasible. As the use of AI quickly evolves, it is important that regulations and standards of AI evolve with it. The purpose of this hearing is to examine the impact of AI in marketing and advertising, consumer privacy and data protections, as well as consumer lending and financing, and examine the role government could play in the regulation of AI to ensure consumer safety and protection. The Committees would like to hear testimony on existing laws and regulations in New York State, other states, or new initiatives being discussed at the state and federal levels regarding the use of AI related to consumer safety and protections.

Submitted Testimonies (organized by panel order)

Panel 1: Chris D'Angelo, Chief Deputy Attorney General for Economic Justice, NYS Office of the Attorney General; Darsana Srinivasan, Health Care Bureau Chief, NYS Office of the Attorney General

Panel 2: Roslyn Docktor, VP, Science and Technology Policy, IBM; Todd O'Boyle, Senior Director of Technology Policy, Chamber of Progress**;** Julie Scelfo, Founder, Mothers Against Media Addiction (MAMA)

Panel 3: Daniel Schwarz, Senior Privacy & Technology Strategist, Policy Department, New York Civil Liberties Union; Beth Finkel, State Director, AARP New York; Casey Mock, Chief Policy & Public Affairs Officer, Center for Humane Technology

Panel 4: David Siffert, Legal Director, Surveillance Technology Oversight Project (S.T.O.P.)

Panel 5: Siwei Lyu, SUNY Empire Innovation Professor, University at Buffalo Department of Computer Science and Engineering; Diane Kennedy, President, New York News Publishers Association & Advertisers Service**;** David Donovan, President and Executive Director, New York State Broadcasters Association

Panel 6: Rebecca Damon, Chief Labor Policy Officer & New York Local Executive Director, SAG-AFTRA; Marjorie Velázquez, VP, Policy, Tech:NYC; Hayley Tsukayama, Associate Director of Legislative Activism, Electronic Frontier Foundation

Testimony of the Office of the

New York State Attorney General Letitia James

Before the New York State Assembly

Standing Committee on Consumer Affairs and Protection

&

Standing Committee on Science and Technology

September 20th, 2024

Good morning. My name is Chris D'Angelo. I am the Chief Deputy Attorney General for Economic Justice at the Office of the New York State Attorney General and I am joined by Darsana Srinivasan who is the Chief of the Healthcare Bureau at the OAG. We look forward to presenting testimony on behalf of the office and answering your questions about this important topic.

The Office of the New York State Attorney General would like to thank Chairperson Rozic, Chairperson Otis, and the committee members for inviting the Office here today to discuss how we can ensure consumer protection and public safety as the use of Artificial Intelligence expands.

Artificial Intelligence is one of the most innovative and consequential advancements in modern technology since the mass production of the personal computer. AI technology has been around for nearly seventy (70) years, but there has been rapid advancement in the field over the past few years.

The new generation of AI, including "Machine Learning AI" and "Generative AI", has become more accessible to a broader range of people and organizations than ever before and is profoundly changing the way we live and work.

Traditional AI is characterized by programmed algorithms and rules, data analysis, restricted applications, formulaic output, and processes limited to specific data defined by a human creator. Traditional AI includes spell check for email or documents, navigation applications, or personalized video recommendations based on your watched content.

Machine Learning AI, which includes Generative AI, is different in many ways.

- Machine Learning AI and Generative AI use large data sets to learn how to perform tasks. For example, a Machine Learning AI may use radiology images to "learn" and train itself to differentiate benign tumors from malignant ones. This differs from traditional AI in that the Machine Learning AI is training itself using a provided data set, it is not using pre-programmed parameters provided by humans.
- Similarly, a Generative AI can create new content based on its learned data rather than simply identifying data. An example of this is image-based Generative AI that creates a unique image

based on a series of word prompts. This is quite different from a search algorithm, which can simply identify existing works that are related to those terms.

- Generative AI can be asked to perform a variety of tasks. An example of this is when a linguistic generative AI model drafts an employment cover letter for one user and summarizes the history of chocolate making for another.
- Machine Learning AI is not limited to specific programmed algorithms but can independently connect, categorize, and use information it has been trained on. Two well-known examples of this process going wrong are Generative AI tools that recommended that users eat a rock a day for good health and use non-toxic glue to keep the cheese from slipping off a slice of pizza. Both of these recommendations were traced back to facetious internet posts that were included in the data set used to train the AI tools. This learning process is why good quality data sets are vital to develop Machine Learning AI, including Generative AI.

There must be continued vigilance regarding AI, especially as AI capabilities grow and the technology becomes ever more pervasive. We also must ensure that New Yorkers' rights, privacy, and human dignity are not threatened by emerging technologies or their implementation.

These new advances present opportunities to improve our lives by accelerating decision-making and reducing human error, but they also present significant risks. Our role as policy makers and enforcer is to assess how we can support innovation while mitigating those risks. While some might argue for a "wait and see" approach to such a new industry, we do not believe we should shy away from taking measured steps to regulate simply because there is complexity or uncertainty. And we do not believe that there is an inherent conflict between growth and innovation on the one hand and smart regulation on the other.

We also know that -- because this technology can be used differently across different industries -- there may not be a one-size-fits-all approach to govern the use of Machine Learning AI and Generative AI. That said, there are some general principals that can help us govern AI in its various applications.

It is apparent that the spread of AI throughout workspaces, homes, and society comes with its share of risks. Chief among them is the risk to civil rights posed by AI's replication and perpetuation of biases and discrimination and its use of incomplete or inaccurate data across industries. Specifically, concerns have been raised about AI that can:

- manipulate personalized advertising and take advantage of consumers, including minors, when marketing products;
- create targeted scams;
- reinforce racial profiling and the disproportionate targeting of minority communities by law enforcement;
- discriminate in hiring and limit economic opportunities;
- deny or charge housing applicants more for rental housing;
- misdiagnose patients and limit appropriate health care treatments; or
- deceive or confuse voters during elections.

On this last point, this month our Office issued a Guide to protect New York voters from AI-generated election misinformation. It provides important information to improve the public's media literacy in the face of sophisticated "deepfakes" and chatbots. It is attached to this testimony (and is available at the following URL: https://ag.ny.gov/publications/protecting-new-york-voters-ai-generated-election-misinformation).

But we also know that there is great potential in the utilization of Artificial Intelligence to improve our lives. It can be used to uplift New Yorkers, address systemic inequities, and create new sectors of employment and economic progress.

In April 2024, the Office of the Attorney General hosted a symposium titled The Next Decade of Generative AI: Fostering Opportunities While Regulating Risks. We gathered experts from academia, advocacy organizations, industry, and policymaking to have an in-depth discussion on how New York could ensure that AI is developed responsibly and for the benefit of everyone.

A copy of the report we issued following that symposium is attached to this testimony (and is available at the following URL: https://ag.ny.gov/sites/default/files/reports/oag-aisymposiumreport.pdf).

Some of the primary concerns that emerged from those discussions included ensuring that:

- AI tools are properly developed and tested to ensure that they are accurate when processing data for all consumers;
- All consumers have equal access to AI tools;
- AI tools are not used to create deceptive deepfakes that can be used to defraud the public or individuals;
- AI corrects for, instead of amplifying, the bias in its training data;
- AI outputs are audited for accuracy and to confirm their outputs are not biased;
- High quality AI training data is not locked up in exclusive contracts so all entities can fairly compete in the AI marketplace;
- AI is not trained on private data; and
- AI tools do not leak personal information.

Some of these goals can be achieved with our current laws and regulations. But others will require new laws or legislation to update current law.

First, transparency. Consumers need to know when they are interacting with AI tools and when companies are using AI to make important decisions about them.

Second, review. Companies must provide a pathway for consumers to request the review of important decisions made by AI when they believe that the underlying data is wrong or the result is inaccurate.

Third, reporting. Companies must provide a way for consumers to report issues, such as hallucinations, with AI tools used in sensitive or high-risk contexts, like healthcare.

Fourth, auditing. AI outputs for important decisions must be regularly audited according to generally accepted standards to ensure that they are fair, accurate, and legal.

Fifth, identification. We need watermarks and other tracking technology to determine whether content is authentic or has been altered or created by AI.

Sixth, data privacy and security. Private consumer data must be protected and must not be able to be reverse engineered to identify the individual.

Ultimately, companies have an obligation to protect others when they use AI, including responsibility for the use of harmful algorithms.

It's particularly important that government agencies, as they incorporate AI as a tool for their work, take special care to address the risks identified here and serve as a model for careful adoption.

Finally, before concluding, we would be remiss not to emphasize that the risks presented by AI highlight the importance of amending New York's deceptive acts and practices law (General Business Law § 349) to expand protections against unfair and abusive conduct and bring our state in line with the 41 other states that already provide stronger protections for their own residents. As in other contexts such as deed theft, housing, and consumer fraud, protections against unfair and abusive conduct would help protect consumers and small businesses against some of the most likely abuses of AI. We strongly encourage the legislature to pass these protections for New Yorkers and offer our partnership in helping to get a bill passed.

Thank you for this opportunity to provide testimony. The Office of the Attorney General looks forward to continuing to work with the committees as the legislature considers regulatory and legislative tools to ensure consumer and public protection relating to the use of Artificial Intelligence.

Testimony of Roslyn Docktor

Vice President, Technology and Science Policy

IBM

Before the

Committee on Consumer Affairs and Protection

New York State Assembly

Hearing on "Ensuring Consumer Protection & Safety Relating to the Use of Artificial Intelligence"

Friday, September 20th, 2024

IBM deeply appreciates the opportunity to testify before this joint hearing of the New York State Assembly Committee on Consumer Affairs and Protection and the Committee on Science and Technology.

IBM in New York State

For our entire 113-year history, IBM has been a proud New York technology company. Today, IBM is a global leader in hybrid cloud and artificial intelligence, providing technology to Fortune 500 companies, governments, and clients in nearly every sector of the global economy. IBM designs, manufactures, markets, and sells many of those leading-edge technology solutions right here in New York State. That includes testing and prototyping chips for the next generation of IBM technology in the Hudson Valley at the Albany Nanotech Center, and pioneering breakthroughs in AI at the headquarters of IBM Research in Yorktown Heights. IBM's most recent high-end chips are designed to accelerate AI processing at the most fundamental level. Our long heritage of leadership in the state continues to this day, with our Chief Executive Officer, Arvind Krishna, proudly co-chairing Governor Hochul's Emerging Technology Advisory Board and having just recently introduced our flagship New York City office at One Madison Avenue, alongside the Governor and U.S. Senate Majority Leader Schumer.

IBM also is a major partner and technology provider to many of New York's state government agencies, and has been engaged in generative AI assessments and initiatives across the state. Both as a leading New York technology company, and a partner to many state agencies, IBM believes that AI can help propel New York's economy forward into the future, this includes the use of AI in many settings that can make business and government smarter, more efficient, and more responsive, and unlock scientific discovery.

IBM & AI

IBM has a long history of helping enterprises, including in New York's robust financial sector, harness artificial intelligence technologies to unlock business value in ways that are responsible and strengthen trust. Our leadership in AI ranges from helping clients identify appropriate use cases, co-creating with clients the solutions to realize their potential, and providing the tools needed to govern both the development and deployment of AI systems.

More recently, breakthroughs in generative AI, which includes large language models, have justifiably ignited considerable excitement around the potential AI holds for business. Our clients are using AI to fight fraud, accelerate drug discovery, address climate change and improve supply chains. But this technology must be developed responsibly, using the same core principles we follow in developing any powerful new innovation.

We must identify the risks associated with AI use cases, and then continuously advance the technology to mitigate those risks. Robust tools that allow businesses to identify potential problems, resolve them, and monitor AI in deployment throughout its lifecycle will ensure standards of care are met, so the world's societal safeguards can match the pace of technological advancement.

IBM values the opportunity to inform the legislative process on AI in New York and in other states. We supported thoughtful AI legislation in Connecticut earlier this year and have been actively working to educate legislatures in capitals across the country. We also recognize that since AI is still rapidly evolving, regulatory proposals will often struggle to balance mitigating risk with fostering innovation. We firmly believe mitigating risk and maximizing innovation can coexist. So, across all of those discussions, IBM has consistently advocated for responsible and

trusted AI adoption. We applaud the Assembly for exploring how government can foster responsible adoption of artificial intelligence in ways that effectively balance protections for individuals while fostering innovation and competitiveness.

Like any technology, AI has the potential to greatly benefit society, but in order for those benefits to be realized, it must be utilized responsibly and transparently. We urge you to focus on three key aspects that IBM recommends policymakers worldwide consider when crafting smart and thoughtful AI legislation. First, the promise and potential of AI technologies. Second, the current guardrails and best practices in place. And, lastly, how regulation can help address any gaps.

AI BENEFITS

The potential of AI for businesses, governments, consumers, and our national economy and security is staggering. Large language models are "foundational" AI models capable of understanding and generating content to perform a wide-range of tasks; much like an AI Swiss army knife, this makes them useful for many different use cases and in many domains. This is a leap forward from previous generations of AI, which required substantial additional effort for each new use case.

At the same time, the conversational abilities of these models allow for a broader range of the workforce to engage with AI systems, which enhances the overall impact. We are at the tip of the iceberg with these impacts and the advancement of large language models and corresponding technologies. As we discuss existing guardrails and gaps, we must keep in mind these benefits and the enormous potential of AI to boost New York State's economy.

The Assembly has recognized this potential by including funding in the NY State Budget to establish the New York Empire AI Consortium. The goal of the Consortium is to allow researchers, public interest organizations, and small companies to gain efficiencies of scale not able to be achieved by any single university, to attract top faculty and expand educational opportunities to NY State, and to give rise to a wave of responsible innovation that will significantly strengthen the state's economy.

The benefits are not just in the future. IBM clients are using LLMs and AI today. In a recent pilot, an IBM client realized 30% cost savings from more efficient budgeting and resource allocation. Across the globe, IBM is implementing a variety of use cases in government, from summarizing contracts to protecting sensitive citizen data.

CURRENT GUARDRAILS / BEST PRACTICES

Over the past century, IBM has cultivated a strong reputation as a trusted technology company. As we advance into the era of AI, we remain committed to maintaining that reputation by leading in industry best practices for responsible technology.

For our entire history, we have focused on managing the societal risks of new technologies that we bring to market. For example, we were among the first companies to establish an AI Ethics Board. The Board, now celebrating 5 years in operation, plays a critical role in overseeing our internal AI governance process and creating internal guardrails to ensure we introduce technology into the world responsibly and safely. The Board provides centralized governance and accountability while still being flexible enough to support decentralized initiatives and business engagements across IBM's global operations.

Trusted

Curating data that goes into training a model is an important undertaking, which should not be taken lightly. For IBM models, we take data curation seriously, applying AI-based content filters designed to remove objectionable material, along with rigorous filtering procedures and blocklists designed to avoid problematic data. We also make substantial efforts to proactively *add* trusted data sources, for instance, in the domain of finance, to ensure that models are trained with high-quality, authoritative information.

Transparency is a cornerstone of trust, so we disclose data sources used in the training of our models. IBM's models have emerged at the top of the rankings among peer model providers.[1]

In brief, we believe that information about data used to train underlying models should be shared with those using the models, especially when it comes to industries that deal in sensitive, personal or heavily-regulated information.

Targeted

The trend toward larger models can increase both resource usage and cost. As a result, there have been counter-trends toward creating smaller models with more focused capabilities. While some model builders have followed a strategy of one omni-capable model to rule them all, we believe that most real-world applications would be better served by "just right"-sized models whose capabilities are well-matched to their needs. A bank customer service chatbot does not need to know how to solve physics problems, and in fact it is inefficient when that chatbot utilizes a larger, more resource-intensive model.

[1] https://crfm.stanford.edu/fmti/May-2024/index.html

Open

The third pillar of IBM's approach to enterprise models is openness. There is a tension between proprietary model developers, who typically keep their models carefully guarded, and open model providers, who (in varying degrees) make their models available to the external community to work with directly. The divide between proprietary and open technology is hardly new, and the current moment is reminiscent of the early days of the internet, when proprietary software providers battled against open-source software. But we need not cast this debate as a binary choice between one or the other. Open models and proprietary models can, and should, coexist within the broader AI marketplace, and businesses and consumers should be able to make their own choice without policy pressing a thumb on the scale against open.

AI POLICY RECOMMENDATIONS

Policymakers and industry players have equally important roles to play in ensuring that AI's increasingly pervasive use does not create unacceptable risks for people and their wellbeing. Policymakers are right to take steps to mitigate the risks of new technologies that are not addressed in current laws, and IBM has long advocated for smart AI policy to address these risks. This approach means leveraging rules that target particular AI use cases, rather than regulating the underlying technology itself. In particular, we advocate for rules that:

Regulate AI risk, not AI algorithms. AI is a tool, and like any tool it can be misused, whether intentionally or unintentionally, in the same way that a hammer can be used to construct a home, or as a weapon. But we do not regulate the underlying tools – we regulate how they are used in different contexts. AI should be no different.

AI can be used in many ways across industries and the entire economy, which is why it is so important to regulate *use*. Rather than focus on regulating the AI algorithms, policymakers should look at those situations in which the use of AI may be considered "high-risk" and whether it is making a "consequential decision" that impacts an individual's fundamental rights. The greatest regulatory control should be placed on the specific uses of AI that pose the greatest risk to people and their wellbeing.

Hold AI developers and deployers accountable. Legislation should consider the different roles of AI developers and deployers and hold them accountable in the context in which they develop or deploy AI. For example, companies using AI for employment decision-making cannot claim immunity from employment discrimination charges. Similarly, if a software developer creates a financial algorithm that promotes fraudulent activities, they should be held liable for the potential harm it may cause. Let's learn from past mistakes with emerging technologies. Section 230 stands as a cautionary tale; we cannot create another broad shield against legal liability. It is essential to find the right balance between innovation and accountability.

Those developing and deploying AI should also be cautious of training an AI system on data with bias. Historical or representational bias could lead to biased or skewed outputs that can unfairly represent or otherwise discriminate against certain groups or individuals. In addition to negative societal impacts, business entities could face legal consequences, disruption to operation, or reputational harms from biased model outcomes.

Support open AI innovation, not an AI licensing regime. Existing regulators are well-positioned to handle most harms associated with AI. We do not need new

agencies to pre-approve or license the development or use of AI. Instead, we should prioritize efforts that keep the AI marketplace competitive, and not unduly preference proprietary AI over more open, readily available models. Further, certain proposals to address the safety risks of AI – such as creating an AI licensing regime – are not helpful. These proposals would impose significant constraints on open innovation in AI, limit competition and innovation in the marketplace, and even jeopardize safety and security. Instead, policymakers should focus on regulating the use of AI, based on risk, regardless of whether the underlying AI model is open or closed.

It's also important to consider the full spectrum of AI use cases and the societal implications, promoting a balanced framework that address legitimate concerns. If not sufficiently targeted and precise, regulatory measures aimed at addressing harm caused by social platforms, for example, could inadvertently create barriers for businesses to utilize AI in low risk, non-consumer applications.

Finally, policymakers should advance the science of AI, including AI risk. Continued support for Empire AI can put New York State at the forefront of this vital work, and promote the sharing of technical resources and other inputs to enable broader collaboration in developing and using AI for the public benefit. IBM Chairman and CEO Arvind Krishna further explains steps government and companies should take to foster trusted and responsible AI adoption here.

THE IMPORTANCE OF OPEN INNOVATION

We would not be at this moment in AI if it were not for the diverse scientific and technical community that has openly contributed for decades to the fundamental advances that we benefit from today. The broad economic and social benefits of

openness are overwhelming. An open AI ecosystem is dramatically more innovative, inclusive, and competitive than a closed one.

- It lowers the barrier to entry for competition and innovation.
- Making technical resources necessary to develop and deploy AI more accessible, open ecosystems enable small and large firms and research institutions to develop new and competitive products and services without potentially prohibitive, upfront costs.
- Openness also drives democratization, which can mean more opportunities for anyone to explore, test, modify, study, and deploy AI, lowering the bar for deploying AI for socially beneficial applications.
- Lastly, it is much easier to learn about a subject when you readily access the materials. An open innovation ecosystem unleashes a significantly broader pool of AI talent, as students, academics, and existing members of the workforce can more easily access the resources necessary to acquire AI skills.

Just as a collaborative AI environment can increase innovation and unlock talent, this regulatory process can do the same. We appreciate your engagement with industry, academia, and others to ensure rules are fit-for-purpose and do not inadvertently hurt innovation. We elaborate on the value of Open AI Innovation here.

Conclusion

At IBM, we have a long history of ushering new technologies into the world in a considered, thoughtful, and intentional manner. We recognize that our license to operate is provided by society, and that we have an obligation to live up to the standards and expectations we have built over the past century of operations. This is particularly true when it comes to developing AI. The need to promote trust in this powerful, and evolving, technology is at an inflection point.

As the members of these committees consider future legislation, we urge all policymakers to focus on the benefits that AI heralds – not only for business, but government and society more generally – and to craft guardrails that address real-world harms, differentiate between developers and deployers, and plug gaps that existing regulations do not cover.

We thank you for the opportunity to submit this testimony, and look forward to working with members of the committees to ensure AI is beneficial to the many, and not merely the few.

CHAMBER OF PROGRESS

Testimony of Todd O'Boyle
Senior Director, Technology Policy
Chamber of Progress

September 20, 2024

Good morning Chair Rozic, Chair Otis and members of the Committees on Consumer Affairs and Protection and the Committee on Science and Technology:

Thank you for the opportunity to testify regarding the best approach to consumer protection and artificial intelligence (AI). On behalf of the Chamber of Progress, a tech industry association supporting public policies to build a more inclusive society where all people benefit from technological advances, I encourage you to embrace sector-by-sector regulation targeting specific consumer harms.

Our organization works to ensure that everyone benefits from technological progress. Our corporate partners include companies like Apple and Midjourney, but our partners do not have a vote on or veto over our positions.

Regulate harms, not technology

The Committees have asked for suggestions on how to protect consumers across a broad range of topics, including marketing, consumer privacy, and lending. We applaud your ambition and thank you for engaging industry for our perspective. Given the breadth

of topics we encourage you to craft sector-specific policies at the application layer that address specific policy goals individually instead of writing an omnibus AI bill.

1. Existing statutes can be updated or tweaked to address AI concerns;
2. AI's impact is different across sectors, and the optimal regulatory approach for one may not hold for another;
3. In areas where the impact of AI is still coming into focus, more study may be called for, but in areas such as the use of AI in advertising, pro-consumer measures are already coming into focus.

Updating existing statutes is more straightforward

2024 has been a year of unprecedented legislative interest in AI. And with reason: AI may transform public education, reshape the labor market, and catalyze the development of new medical treatments.

With more than 800 bills introduced in legislatures so far this year, several themes have emerged. One is that rigorously defining "artificial intelligence" proves much trickier than imagined. As a practical matter, many of the proposed definitions suffer from one of two flaws: either they define AI by reference to an arbitrary level of computing power - which is subject to immediate obsolescence thanks to continued technological advance. Or they define AI based as software that "mimics tasks typically performed by human cognition." In this case, they unintentionally cast such a wide net that most consumer software - like spell check and spreadsheets - ends up in scope.

A better approach is to identify a specific harm—such as housing discrimination—and update existing New York statutes to close any AI loopholes. This approach avoids arbitrary technological thresholds and obviates the challenges of strictly defining AI. In essence, it is more seamless and futureproof. This approach also allows you to better utilize AI to tackle challenges on the minds of everyday New Yorkers, like affordable housing, access to well-paying jobs, and safeguarding New York's environmental health and green spaces.

The right approach varies greatly

AI in advertising presents unique challenges. Above all, in an election year when generative AI can be used to create deceptive imagery, audio, or video that can misinform the electorate.

Thankfully, private sector innovation is helping lead the way for transparency. Earlier this year, shady actors sent robocalls in New Hampshire with an audio deepfake of President Biden discouraging participation in the primary. Almost immediately, Pindrop used its audio deepfake detection engine to determine how it was created - critical forensic clues.

As useful as that is, more transparency may be necessary, particularly in political communications. To that end, we encourage you to take a medium-neutral approach. In other words, disclosure of the use of AI in advertising should be required across media - whether digital, print, or otherwise. We further note that penalties for non-compliance should rest with the advertiser alone. In short, sound policy targets the bad actor, not the tool being manipulated.

More study is necessary is many areas

Lastly, we value consumer privacy and support strong national privacy protections. However, the interplay between consumer privacy and artificial intelligence is still coming into focus. Legislators in several states have considered mechanisms to allow consumers to opt out of their data being used to train AI. The technical feasibility of doing this consistently and at scale is unproven, and even if those challenges can be overcome, you risk creating a scenario in which developers have to maintain separate codebases - one for New York and one for the rest of the country. That would chill New York's vibrant startup ecosystem and may slow the pace at which new products are brought to market here. Accordingly, we urge you to study this issue, as the industry, civil society and end users work towards best practices on privacy and AI.

Thank you, and I look forward to your questions.

Ms. Julie Scelfo
September 20, 2024
Re: NYS Assembly Legislative Hearing on Artificial Intelligence and Consumer Protection

Good morning Chairs and Committee members. I am Julie Scelfo here today on behalf of Mothers Against Media Addiction, or MAMA. MAMA is a grassroots movement of parents and allies fighting back against media addiction and creating a world where real life experiences and interactions remain at the heart of a healthy childhood.

I am a resident of New York, a longtime journalist, and the parent of three young New Yorkers. All three of my sons were born in NY, and they are the beneficiaries of New York's rich land and culture, from fishing in the Catskills to eating at food trucks in Brooklyn. My husband and I, along with our families, friends and neighbors, and their many teachers, have done everything in our power to nourish our sons' hearts and minds.

But I'm here today because my children, just like all of NY's children, are being threatened by technology in ways that were unimaginable to previous generations, and we need our lawmakers to act to protect their safety.

Since the advent of digital technology and the Internet, we have been deploying technology at a massive scale, lured by shiny promises from tech companies — without fully considering these products' potential harms.

The CEO of Meta said his products exist to "connect the world." But very little thought was given in advance to how "connecting the world" meant allowing child predators, criminals, hate groups, terrorists, and foreign governments to infiltrate the daily lives of American adults, and our children.

Social media platforms have, for years now, been amplifying harmful content such as self-harm, eating disorders, hate speech, racism and unhealthy beauty standards.

Across New York, and the whole nation, parents today are living with the aftermath of having widely and rapidly adopted those products without our lawmakers *first* making sure they were safe.

Today I'm here to beg you: please don't let that happen again.

Because we allowed the proliferation of smartphones and social media *without* proper safeguards in place we are in the midst of a national emergency in youth mental health. That means elevated rates of youth anxiety, depression, self-harm, suicide, eating disorders and more. Additionally, attention spans are falling and reading and math scores are going down, which has profound effects on our communities, the workforce and our future democracy.

As social media companies' own internal documents show, those problems did not happen by chance. They were the result of intentional data practices and A.I. design choices selected by humans, to maximize profit.

Those choices indeed have been incredibly lucrative for those companies, and for a tiny handful of people who own them. But they represent an assault on our collective humanity, and on children, who deserve to be a protected class.

Today, artificial intelligence products present new opportunities, yes, but they also present such unprecedented risks, that many of the folks involved with designing and building A.I. have been issuing warnings about its danger. Geoffrey Hinton, who is often called "the Godfather of A.I." last year told the *New York Times*, "It is hard to see how you can prevent the bad actors from using it for bad things."

As a parent, when someone who invents a product tells you it's dangerous and that bad actors will use it for bad things? You listen.

And we, the parents at MAMA, hope the lawmakers of this state will listen too. We are already seeing the harms to children from A.I., and we parents need help because the problem is at the product design level.

ChatGPT and other AI products have only been in the public consciousness for about two years but we already see some of the ways it harms kids:

- Children's learning is being compromised. From grade school to universities, GenAI applications are being used to cheat on homework and tests, and there aren't adequate tools to truly check if a student has used these applications.
- Healthy relationships are suffering. Social media companies have begun directly integrating A.I. chat bots to promote increased, personalized engagement— which may seem harmless on its face, but capitalizes on kids' vulnerability and search for companionship.
- Reality is being blurred. Adults are having difficulty discerning whether news, advertisements and even correspondence is real or fake.

    - Imaginary friend chat bots and other role playing bot apps are being marketed to kids with little distinction that these entities are not real.
    - AI mental health chat bots are being marketed as "therapy" despite the bots being unlicensed to provide advice.
- Kids are exposed to harmful content. Chat bots can expose kids to misinformation and/or hardcore pornography, or promote dangerous behavior because the data sets AI companies are using to train their models contain harmful or illegal content, including Child Sexual Abuse Material (CSAM).
- A.I. is aiding the creation of CSAM.
    - Nudification apps, where users input photos of real people and A.I. returns deep fake photos in which the subject of the photo then appears nude. There have been numerous cases in the past year alone of teens and students using these apps to produce sexually explicit images of celebrities, but also their peers — and these apps are marketed towards kids.
- Children are being exploited and deceived, with Generative AI being used to turbocharge sextortion and other cybercrimes, often targeting children.

Children deserve to be safe, and that's why lawmakers have, for decades now, made sure that consumer products are safe. There are product liability laws that ensure cribs and car seats are manufactured to meet safety standards.

There are consumer safety laws that ensure vehicles include seatbelts and we have mechanisms for enforcement.

By law, we don't allow children to purchase liquor, visit casinos or rent pornographic videos.

Why would we allow AI products that introduce those harms to our children, at an unprecedented scale?

In short, keeping kids safe online is something all New Yorkers want, and something this elected body should do *now*. Waiting until more children and families suffer the consequences would be a huge mistake, and a dereliction of our duty to put children ahead of profits.

##

REFERENCES

Davis, Antigone. September 12, 2024. "Preventing Suicide and Self-Harm Content Spreading Online." *FB.com.*
https://about.fb.com/news/2024/09/preventing-suicide-and-self-harm-content-spreading-online/

Metz, Cade. May 1, 2023. "The Godfather of A.I.' Leaves Google and Warns of Danger Ahead". *The New York Times.*
https://www.nytimes.com/2023/05/01/technology/ai-google-chatbot-engineer-quits-hinton.html

Confino, Paolo. September 6, 2024. "No one has gained more wealth this year than Mark Zuckerberg, who is up $56 billion." *Fortune.*
https://fortune.com/2024/09/06/mark-zuckerberg-net-worth-elon-musk-jensen-huang-nvidia-meta-tesla-amazon-jeff-bezos-ceo/

Lima-Strong, Cristiano. July 9, 2024. "In a first, federal regulators ban messaging app from hosting minors." *The Washington Post.*
https://www.washingtonpost.com/technology/2024/07/09/ftc-bans-kids-ngl-messaging-app/

Lomas, Natasha. February 3, 2023. "Replika, a 'virtual friendship' AI chatbot, hit with data ban in Italy over child safety. *TechCruch.com*
https://techcrunch.com/2023/02/03/replika-italy-data-processing-ban/

Metcalf, Michael. Undated. "7 of the best AI mental health chatbots to support you." *GetMarlee.com*
https://getmarlee.com/blog/mental-health-chatbot

Harris, David Evan, and Willner, Dave. August 30. 2024. "Was an AI Image Generator Taken Down for Making Child Porn? An inquiry into models that can create child sexual abuse material may have yielded results." *IEEE.org.*
https://spectrum.ieee.org/stable-diffusion

Knutson, Jacob June 23, 2023. "How AI is helping scammers target victims in 'sextortion' schemes." *Axios.*
https://www.axios.com/2023/06/23/artificial-intelligence-sexual-exploitation-children-technology

Thorn. June 24, 2024. "New Research from Thorn: Financial Sextortion on the Rise, Targeting Teen Boys." *Thorn.com.*
https://www.thorn.org/blog/new-research-from-thorn-financial-sextortion-on-the-rise-targeting-teen-boys/

ACLU of New York

Legislative Affairs
125 Broad Street
New York, NY 10004
212-607-3300
www.nyclu.org

Testimony of Daniel Schwarz

On Behalf of the New York Civil Liberties Union

Before the New York Assembly Standing Committee on Consumer Affairs and Protection and the New York Assembly Standing Committee on Science and Technology Regarding Consumer Protection and Safety Relating to the Use of Artificial Intelligence

September 20, 2024

The New York Civil Liberties Union ("NYCLU") respectfully submits the following testimony on consumer protection and safety relating to the use of artificial intelligence. The NYCLU, the New York affiliate of the American Civil Liberties Union, is a not-for-profit, non-partisan organization with eight offices throughout the state and more than 180,000 members and supporters. The NYCLU's mission is to defend and promote the fundamental principles, rights, and values embodied in the Bill of Rights, the U.S. Constitution, and the Constitution of the State of New York. The NYCLU works to expand the right to privacy, increase the control individuals have over their personal information, increase transparency and accountability in the use of algorithms, artificial intelligence ("AI"), and automated decision systems ("ADS"), and ensure that civil rights and liberties are enhanced rather than compromised by technological innovation.

AI and ADS broadly – software tools or processes that automate, replace, or aid human decision-making – are widely used to administer services, allocate resources, tailor offerings or customize products, and make inferences about individuals, groups, or places. Whether across government agencies or in private businesses, their ubiquity and opaque deployment risk severely undermining the civil, human, and privacy rights of New Yorkers. The use of ADS is often accompanied by an acute power imbalance between those deploying these systems and those affected by them, particularly given that ADS operate without transparency or even the most basic legal protections. Especially where New Yorker's fundamental rights are at stake – such as in welfare, education, employment, housing, health care, finance, insurance, the family regulation system, or the criminal legal system, these technologies all too often replicate and amplify bias, discrimination, and harm towards populations who have been and continue to be disproportionately impacted by bias and discrimination: women, Black, Indigenous, and all people of color, religious and ethnic minorities, LGBTQIA people, people living in poverty, people

with disabilities, people who are or have been incarcerated, and other marginalized communities.

The New York State Legislature must act to provide meaningful transparency and accountability to ADS and ensure they do not digitally circumvent New York's laws against discrimination. Any regulation must cover ADS broadly, mandate comprehensive and impartial impact assessments, require transparency and clear notice to affected people, and provide opportunities to contest the results of such tools as well as viable paths to request reasonable accommodations. New Yorkers should not need to worry about being screened by a discriminatory algorithm when applying for housing, work, or credit; they shouldn't have to fear faulty software tools affecting their health care or education; and they should not be offered different opportunities or choices based on their demographics. To achieve these goals, we provide the Digital Fairness Act, A.3308/S.2277; the Bossware and Oppressive Technology Act (BOT Act), A.9315-A/S.7623-B; and the NY Department of Financial Services AI Circular Letter as exemplary frameworks for consideration by the Legislature as it engages further on issues related to AI and ADS.

The Need for Regulation of Automated Decision Systems

While the use of ADS undoubtedly boosts speed and scale, such efficiency is only valuable if the underlying decisions are desirable. Even with the little public information available about ADS, researchers and experts consistently reveal their failures with respect to accuracy and neutrality. Many studies have challenged their opaque or "black box" operation[1] and provided evidence of harmful,[2] discriminatory,[3] sexist,[4] and racist[5] outcomes.

---

[1] *See e.g.:* CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY (2016); FRANK PASQUALE, THE BLACK BOX SOCIETY (2015).

[2] *See e.g.:* VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR (2018); Ed Pilkington, *Digital dystopia: how algorithms punish the poor*, THE GUARDIAN, October 14, 2019, https://www.theguardian.com/technology/2019/oct/14/automating-poverty-algorithms-punish-poor; Colin Lecher, *A healthcare algorithm started cutting care, and no one knew why*, THE VERGE (2018), https://www.theverge.com/2018/3/21/17144260/healthcare-medicaid-algorithm-arkansas-cerebral-palsy.

[3] SOLON BAROCAS & ANDREW D. SELBST, *Big Data's Disparate Impact* (2016), https://doi.org/10.2139/ssrn.2477899.

[4] *See e.g.:* Jeffrey Dastin, *Amazon scraps secret AI recruiting tool that showed bias against women*, REUTERS, October 10, 2018, https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G; Galen Sherwin, *How Facebook Is Giving Sex Discrimination in Employment Ads a New Life*, AMERICAN CIVIL LIBERTIES UNION , https://www.aclu.org/blog/womens-rights/womens-rights-workplace/how-facebook-giving-sex-discrimination-employment-ads-new.

[5] *See e.g.:* Kate Crawford, *Opinion | Artificial Intelligence's White Guy Problem*, THE NEW YORK TIMES, June 25, 2016, https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html; Alistair Barr, *Google Mistakenly Tags Black People as 'Gorillas,' Showing Limits of Algorithms*, WSJ (2015), https://blogs.wsj.com/digits/2015/07/01/google-mistakenly-tags-black-people-as-gorillas-showing-limits-of-algorithms/.

Software systems are often wrongly perceived as more neutral than humans or as offering a scientific and objective truth.[6] Their proponents are able to make these assertions because the vast majority of ADS are opaque systems, secretly deployed and shielded from independent review due to their proprietary nature. This secrecy obscures the potential errors, outright flaws, biased data, subjective decisions, and personal choices that find their way into these systems. Every ADS is a product of human design, input, and operation. Raji et al. (2022) provide a taxonomy of AI system failures that can also be used to understand types of algorithmic error – including failures or errors stemming from engineering and design processes, post-deployment processes, and communications about AI systems wherein developers make deceptive claims about AI systems' capabilities.[7]

Precisely-targeted pricing, advertising, and other ADS are used to exclude people of color, women, and older individuals from housing, credit, and employment opportunities in ways that would be unthinkable in the offline world.[8] During the 2016 election, personal information was used to target advertisements to Black Americans urging them not to vote.[9] Indeed, privacy violations can lead to a range of harms, from monetary losses to harassment to public exposure of our intimate lives to reputational damage. Misuse and abuse of personal information in the digital age can limit awareness of and access to opportunities, exacerbate information disparities, erode public trust and free expression, and disincentivize individuals from participating fully in digital life.[10]

Unfair and discriminatory ADS have also become pervasive in all areas where New Yorkers' fundamental rights are at stake, including in welfare, education, employment, housing, health care, finance, insurance, the family regulation system, or the criminal legal system. Landlords and property managers use various ADS products that unfairly screen out potential tenants based on past criminal records. The data that they rely on may contain records that are severely outdated and include sealed and expunged records that should not serve as a basis to disqualify tenants. In other instances, they infer such classifications from other data, or they falsely attribute criminal history based on identical names or address history.[11]

---

[6] danah boyd & Kate Crawford, *Critical Questions for Big Data: Provocations for a cultural, technological, and scholarly phenomenon*, 15 INFORMATION, COMMUNICATION & SOCIETY 662–679 (2012).
[7] Inioluwa Deborah Raji et al., *The Fallacy of AI Functionality*, Assoc. for Computing Machinery (June 20, 2022), https://dl.acm.org/doi/abs/10.1145/3531146.3533158.
[8] See Galen Sherwin & Esha Bhandari, *Facebook Settles Civil Rights Cases by Making Sweeping Changes to Its Online Ad Platform*, ACLU SPEAK FREELY, Mar. 19, 2019, https://www.aclu.org/blog/womens-rights/womens-rights-workplace/facebook-settles-civil-rights-cases-making-sweeping.
[9] Natasha Singer, *Just Don't Call It Privacy*, NYTIMES, Sept. 23, 2018, https://www.nytimes.com/2018/09/22/sunday-review/privacy-hearing-amazon-google.html.
[10] *Id.*
[11] Ariel Nelson, *Broken Records Redux: How Errors By Criminal Background Check Companies Continue to Harm Consumers Seeking Jobs and Housing* (Dec. 2019), https://www.nclc.org/wp-content/uploads/2022/09/report-broken-records-redux.pdf; see also Lauren Kirchner & Matthew Goldstein, *Access Denied: Faulty Automated Background Checks Freeze Out Renters* (May 28, 2020),

Obtaining access to ADS's underlying source code and data is difficult and resource intensive, but absolutely critical to understanding the extent to which errors occur and whether they are likely to cause discriminatory harm. For example, it was revealed that a Medicaid ADS in Arkansas had failed to correctly assess care needs of patients with cerebral palsy or diabetes: a fact only discovered through lengthy litigation and subsequent disclosure of the code.[12] And in New York City, an independent review of the source code of a DNA analysis tool used by the Office of the Chief Medical Examiner raised serious questions about its validity, including whether the code may have been intentionally skewed to create more matches.[13]

Many automated systems purport to predict the future by observing the past. Chief among them are "risk assessment tools," designed to use past policing and court data to "predict" the future behavior of an individual criminal defendant. Specifically, risk assessment tools attempt to determine which attributes are shared by people who previously failed to show up to court. Certain weights are placed on each of the attributes to produce a formula and "score" a person's future risk of flight. Risk assessment tools reflect a troubling philosophy toward criminal justice policy: Using past cases to determine what might happen in future cases disregards time-specific influences that may have affected prior case outcomes and freezes a government judgment in the realities of the past. Critically, it also strips the person who is awaiting trial of independent agency and the ability to make the case that they will appear in court.

But even those who philosophically agree with using past statistics to predict future individual human behavior acknowledge that the value of such a predictive system lies in the value of the data input into it. When an ADS deploys machine learning that relies on large historic datasets to train the underlying models, the quality of that underlying data is of paramount importance. If that data includes false or biased data, every output will repeat this pattern and in turn result in false and biased decision-making. In the context of policing, utilizing data from unconstitutional and racially biased stop-and-frisk practices by the NYPD will create outputs reflecting these practices.[14] This behavior is commonly known by the computer-science idiom "garbage in, garbage out," or in this scenario, as Sandra Mayson coined, "bias in, bias out."[15]

In another recent example, researchers discovered that a widely used health care algorithm used to identify patients' health risks failed to identify many Black patients, making

---

https://themarkup.org/locked-out/2020/05/28/access-denied-faulty-automated-background-checks-freeze-out-renters.

[12] Litigating Algorithms 2018, AI NOW INSTITUTE, https://ainowinstitute.org/litigatingalgorithms.pdf.

[13] Lauren Kirchner, *Thousands of Criminal Cases in New York Relied on Disputed DNA Testing Techniques*, PROPUBLICA (2017), https://www.propublica.org/article/thousands-of-criminal-cases-in-new-york-relied-on-disputed-dna-testing-techniques.

[14] Rashida Richardson et al., *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice,* 94 N.Y.U. L. REV. ONLINE 192 (2019), https://ssrn.com/abstract=3333423.

[15] Sandra G. Mayson, *Bias In, Bias Out*, 128 YALE LAW JOURNAL (2019), https://www.yalelawjournal.org/article/bias-in-bias-out. Archived at: http://archive.is/nzP1D.

them less likely to be enrolled for medical treatment.[16] And where these systems operate in the dark, people may not even realize that they are suffering at the hands of a flawed algorithmic system. One ADS in Indiana blocked hundreds of thousands of people from receiving vital support services and left them struggling to challenge these decisions.[17]

Given the enormous human impacts from automated systems – and the very real possibility of simply automating existing human error and bias – meaningful regulation is the bare minimum our democracy demands. The growing power imbalance between people affected by ADS and those who deploy them is at its height when affected people are not even aware that their lives have been impacted by an ADS.

A bill in the New York Legislature, the **Digital Fairness Act, A.3308/S.2277**, would address many of the tangible harms that arise from the abuse and misuse of personal information in the digital age by making clear that it is both unlawful discrimination and an unfair trade practice to use personal information to circumvent our civil and human rights laws. It would create comprehensive privacy protections by requiring meaningful notice and affirmative, opt-in consent from people before their personal information is captured or used, as well as heightened protections for biometric information, and provide people with the ability to access and delete their personal information and to transfer their personal information to another company. In addition, it would provide guardrails for government use of ADS. It would ban discriminatory tools and require that any governmental ADS undergo and pass a civil rights audit conducted by a neutral third party before it is deployed. It would also require that individuals subjected to government automated decisions receive notice of the decision made, the involvement of an automated system, and an opportunity to contest the decision and seek human review. And the bill would require government entities that use automated decision-making systems to have appropriate governing policies in place, adhere to transparency requirements, and have the approval of the relevant governing body – following a public hearing – before acquiring any new systems. The Digital Fairness Act is a comprehensive solution to tackle the worst harms of digital technologies by protecting privacy and addressing the civil rights abuses associated with misuse and abuse of personal information. **The NYCLU strongly supports this legislation**.[18]

---

[16] *See:* Beth Haroules & Simon McCormack, *How an Algorithm Puts Black People's Health in Danger*, NEW YORK CIVIL LIBERTIES UNION (2019), https://www.nyclu.org/commentary/how-algorithm-puts-black-peoples-health-danger; Ziad Obermeyer et al., *Dissecting racial bias in an algorithm used to manage the health of populations*, 366 SCIENCE 447–453 (2019).

[17] Alyssa Edes & Emma Bowman, *"Automating Inequality": Algorithms In Public Services Often Fail The Most Vulnerable*, NPR.ORG (2018), https://www.npr.org/sections/alltechconsidered/2018/02/19/586387119/automating-inequality-algorithms-in-public-services-often-fail-the-most-vulnerab; Virginia Eubanks, *We created poverty. Algorithms won't make that go away*, THE GUARDIAN, May 13, 2018, https://www.theguardian.com/commentisfree/2018/may/13/we-created-poverty-algorithms-wont-make-that-go-away.

[18] *See:* Legislative Memorandum - Digital Fairness Act, A.3308 / S.2277, NYCLU (2024), https://www.nyclu.org/uploads/2023/12/2023-2024-legislativememo-digitalfairnessact.pdf.

A particular area of concern is the use of ADS in the employment context. Here, too, ADS are widely used; yet their operation is shrouded in secrecy, and they risk undermining existing labor and civil rights protections.[19] Examples abound with racist, sexist, ableist, or other biased ADS, with resume scanners that prioritize male candidates,[20] systems that are inaccessible to applicants with disabilities,[21] and racially biased video interview platforms.[22] To stop these practices from occurring, **the Bossware and Oppressive Technology Act ("BOT Act"), A.9315-A/S.7623-B**, would require employers to conduct impartial impact assessments that assess the validity of these tools, their potential for disparate impact on any protected class and potential remedies to address those impacts, and their impact on accessibility for people with disabilities. Employers would be required to publish the results of these assessments in a public registry. The bill would also mandate meaningful notification regarding the use of ADS, alternative selection procedures, requests for human review, appeals processes, and clear prohibitions of tools that violate laws, threaten welfare, or have discriminatory impact.

The BOT Act incorporates lessons learned from prior efforts to address discriminatory algorithms in the workplace. New York City attempted to tackle bias in ADS by enacting Local Law 144 of 2021 ("LL144"). Unfortunately, this measure fell far short of providing comprehensive protections for job candidates and workers.[23] LL144 requires employers to conduct what amounts to little more than severely limited bias audits of only a narrow scope of tools they use and only share certain results of these already inadequate audits publicly. It also fails to provide workers with the information they need to meaningfully assess the impact an ADS has on them and whether they need to request an alternative selection process or accommodation; does not ensure there are alternative selection procedures; does not prohibit technologies with discriminatory impact; and lacks sufficient enforcement mechanisms. More than a year after LL144 came into effect, it has become abundantly clear that it is far too weak to protect against bias and to hold employers and vendors accountable.[24] In contrast to A.9315-A/S.7623-B, it also does not include any protections against workplace surveillance. All these gaps and loopholes – to say nothing of the lack of even these minimal protections outside of New

---

[19] Olga Akselrod & Cody Venzke, *How Artificial Intelligence Might Prevent You From Getting Hired*, AMERICAN CIVIL LIBERTIES UNION (Aug. 23, 2023), https://www.aclu.org/news/racial-justice/how-artificial-intelligence-might-prevent-you-from-getting-hired.

[20] Jeffrey Dastin, Amazon scraps secret AI recruiting tool that showed bias against women, REUTERS, October 10, 2018, https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G.

[21] Lydia X. Z. Brown, Ridhi Shetty & Michelle Richardson, *Report – Algorithm-Driven Hiring Tools: Innovative Recruitment or Expedited Disability Discrimination?*, CENTER FOR DEMOCRACY AND TECHNOLOGY (Dec. 3, 2020), https://cdt.org/insights/report-algorithm-driven-hiring-tools-innovative-recruitment-or-expedited-disability-discrimination/.

[22] Ifeoma Ajunwa, *Automated Video Interviewing as the New Phrenology*, (2021), https://papers.ssrn.com/abstract=3889454.

[23] Daniel Schwarz, *Testimony Regarding Tackling Bias in Automated Employment Decision Tools*, NYCLU (2022), https://www.nyclu.org/resources/policy/testimonies/testimony-regarding-proposed-rules-implement-local-law-144-2021-tackling-bias-automated.

[24] Daniel Schwarz & Simon McCormack, *Biased Algorithms Are Deciding Who Gets Hired. We're Not Doing Enough to Stop Them*, NYCLU (2023), https://www.nyclu.org/commentary/biased-algorithms-are-deciding-who-gets-hired-were-not-doing-enough-stop-them.

York City – underscore why the BOT Act is urgently needed, and **the NYCLU strongly supports its passage**.[25]

The Legislature should also look to the guidance by the Department of Financial Services (DFS), which issued a circular letter on the use of artificial intelligence systems and external consumer data and information sources in insurance underwriting and pricing in July 2024.[26] The letter emphasizes that insurers must ensure that their use of ADS does not result in unfair or unlawful discrimination against protected classes. Insurers are required to demonstrate that their data and models show validity and have a clear, empirical relationship to risk. The DFS mandates comprehensive assessments, including proxy assessments,[27] to identify and mitigate any disproportionate adverse effects on protected classes. Insurers must implement robust governance frameworks, including board oversight, documented policies and procedures, and regular audits of their AI and data usage. The letter stresses the importance of transparency, requiring insurers to disclose their use of AI and consumer data to impacted people. In cases of adverse decisions, insurers must provide detailed reasons, including all information upon which the decision was based and the source of that information; and they must provide a process for the applicant to review the accuracy of the data.

The NYCLU urges the Legislature to look to these bills and the DFS guidance as guiding frameworks for its approach to AI and ADS. It is imperative that the Legislature enacts legislation that will serve our democratic values and create the regulatory mechanisms necessary to protect against harmful and discriminatory algorithms across issue areas and industries. Effective regulation will necessarily include mandatory, independent racial, disability, and non-discrimination impact assessments; data privacy audits; and holistic consultation with domain experts and people directly affected by the consequences of any ADS – in particular from marginalized groups – prior to any ADS rollout and throughout the entire life cycle. The Legislature must recognize that technologies showing significant discriminatory impact against any class protected under the New York Human Rights Law, as well as systems that pose high risks of discrimination – e.g. biometric surveillance, analyzing facial features or movements, body language, emotional state, affect, personality, tone of voice, or pace of speech – require outright bans or moratoria.

---

[25] *See:* Legislative Memorandum - Bossware and Oppressive Technology Act, A.9315-A / S.7623-B, NYCLU (2024), https://www.nyclu.org/uploads/2024/05/2024-LegMemo-BOTAct.docx.pdf.

[26] New York Department of Financial Services, Insurance Circular Letter No. 7, July 11, 2024, https://www.dfs.ny.gov/industry-guidance/circular-letters/cl2024-07.

[27] The American Academy of Actuaries has noted that "algorithm[s] may learn to identify and rely upon seemingly facially neutral variables that have a close correlation to protected characteristics or traits" and that such "problematic proxy variables . . . may cause protected classes to be disparately impacted[.]" American Academy of Actuaries, Discrimination: Considerations for Machine Learning, AI Models, and Underlying Data (Feb. 2024), https://www.actuary.org/sites/default/files/2023-08/risk-brief-discrimination.pdf.

Conclusion

The NYCLU thanks the Committees for the opportunity to provide testimony and for recognizing the need for consumer protections for the use of AI and automated decision systems. The NYCLU urges the Legislature to pass legislation to create transparency and protections ensuring fair and equitable use of automated decision systems, particularly in areas where New Yorkers' fundamental rights are at stake – such as in welfare, education, employment, housing, health care, finance, insurance, the family regulation system, and the criminal legal system.

Thank you for your attention to these matters. For any questions or further discussion, please contact Daniel Schwarz, Senior Privacy & Technology Strategist, dschwarz@nyclu.org.

AARP New York

Testimony before the

Assembly Standing Committee on Consumer Affairs and Protection

Assembly Standing Committee on Science and Technology

Ensuring consumer protection & safety relating to the use of artificial intelligence

September 20, 2024

Good afternoon. I'm Beth Finkel, the State Director for AARP New York. AARP is a social mission organization with 2.2 million members in the state, and we advocate on behalf of all New Yorkers age 50 and older. Thank you for the opportunity to comment on the important issue of consumer protections in the use of artificial intelligence. AARP policy supports strong consumer privacy protections across sectors including health, employment and housing. We believe policymakers and the private sector have a key role to play in preventing the misuse of personal information and ensuring consumers are not victims of bias or discrimination.

Algorithmic decision tools powered by artificial intelligence are being used for consequential decision-making in a variety of contexts. These decisions include who is offered a job; who receives access to credit, insurance, and other financial products; who receives health services; and who is eligible for government benefits. AI can bring significant benefits to many sectors. It can improve mobility, increase quality and efficiency in health care, and expand access to financial services. It can also reduce complexity and inefficiency in consumer interactions. But without safeguards, these decision-making tools can produce results that are biased, reflecting historic and ongoing societal prejudices, including against older adults.

The challenge for all of us is how to support the potential benefits of AI while ensuring fairness, transparency, and accountability for consumers. One area of real concern for AARP is fraud.

The issue of fraud is one that seriously impacts older adults, and fraud is now at a crisis level in America. The Federal Trade Commission's (FTC) latest data[1] shows there were $10.3 billion in fraud losses in 2023 – a dramatic increase from the $1.9 billion in losses in 2019. The Federal Bureau of Investigation's (FBI) numbers are even more stark. In 2023, the FBI reported

[1] https://public.tableau.com/app/profile/federal.trade.commission/viz/ConsumerSentinel/Infographic

$12.5 billion in losses (compared to $3.5 billion in 2019). And because fraud is vastly underreported, this likely only represents a small fraction of total losses. An AARP study in 2021[2] estimated 9 in 10 Americans encountered a fraud attempt, and 1 in 7 had money stolen from them in 2020 alone.

While the issue of fraud is not unique to older adults, it often has a disproportionate financial impact on them. According to FTC data, older adults reported higher median losses than younger adults in 2023, with a median loss of $1450 for those age 80-plus reporting a fraud loss, compared to $460 for those in the 20-29 age group. Older adults are often targeted by criminals because they have more money – they have had a longer time to accumulate savings and are therefore appealing targets for criminals. These losses can have significant impacts on the financial security of older adults, as they are often living on fixed incomes and cannot afford to lose funds to criminals.

Artificial intelligence can give criminals the tools to create new and sophisticated scams. Scammers can use deepfake technology such as AI-generated audio and video to impersonate people, gaining access to bank accounts or convincing older adults to send money. The prevalent "grandparent scam," where a fraudster will call an older adult pretending to be a grandchild urgently in need of money, can now be all the more convincing with the use of voice-cloning technology[3]. AI can make it harder for even the most careful older adult to spot a scam.

To help combat this issue, AARP has been monitoring a number of measures on the federal level:

[2] https://www.aarp.org/pri/topics/work-finances-retirement/fraud-consumer-protection/fraud-victim-susceptibility-study.html

[3] https://states.aarp.org/arizona/chatbots-and-voice-cloning-fuel-rise-in-ai-powered-scams

- The **Preventing Deep Fakes Scam Act,** which AARP has endorsed, would establish a federal task force to examine the effects of AI on the financial industry. The task force would include a panel of experts on financial services and AI technology to examine how scammers are using this technology, and look at ways the industry can use AI to better detect scams and fraudulent activity[4].
- AARP has also endorsed the **Learn AI Act**, which would create a national strategy to improve technical literacy of American consumers to safely engage with AI. This legislation would bring together federal agencies with key industry experts and stakeholders to create a literacy campaign.
- President Biden issued an executive order[5] on Safe, Secure, and Trustworthy Artificial Intelligence. The order requires more transparency from technology developers and will establish standards to ensure AI is trustworthy and secure. It also establishes guidance for content authentication to protect Americans from AI-generated fraud.

We welcome the opportunity to work with you and others here in New York to ensure a balanced and safe approach to the use of artificial intelligence. I thank you again for the opportunity to testify and I welcome your questions.

[4] https://www.aarp.org/politics-society/advocacy/info-2024/deepfake-scams-financial-industry.html#:~:text=To%20help%20tackle%20the%20problem,on%20the%20financial%20services%20industry.

[5] https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/

SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

40 Rector Street, 9th Floor
New York, New York 10006
www.StopSpying.org | (212) 518-7573

STATEMENT OF
DAVID ALFASI SIFFERT, ESQ.
LEGAL DIRECTOR
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT ("S.T.O.P.")

BEFORE THE
ASSEMBLY STANDING COMMITTEE ON CONSUMER AFFAIRS AND PROTECTION AND ASSEMBLY STANDING COMMITTEE ON SCIENCE AND TECHNOLOGY

FOR A HEARING CONCERNING
CONSUMER PROTECTION AND SAFETY RELATIN TO THE USE OF ARTIFICIAL INTELLIGENCE

PRESENTED
SEPTEMBER 19, 2024

Chair Rozic, Chair Otis, and members of the Standing Committees on Consumer Affairs & Protection and Science & Technology,

Thank you for inviting me here to address you today. The rapid increase in the prevalence of artificial intelligence has important implications for New York State, and I am very happy to see your committees taking the issue seriously and holding this hearing to learn more.

I will make three points in these remarks: First, artificial intelligence poses a risk to consumers' civil rights. Second, artificial intelligence systems are often sold under false pretenses, posing a risk of fraud to those looking to purchase such systems. Third, AI deployment creates increasingly severe privacy concerns for consumers that can be exploited to target pregnant people, protesters, undocumented New Yorkers, or parents seeking gender-affirming healthcare for their children.

Civil Rights Risks

New York's consumers are increasingly subjected to AI during their attempts to make simple purchases. For example, New Yorkers looking to buy groceries are increasingly likely to face grocery store cameras equipped with facial recognition technology. As another example, consumers of housing looking to rent an apartment are likely to have their applications screened by AI algorithms. Most recently, companies are developing "dynamic pricing" systems with digital price tags, allowing a store to update prices hundreds, thousands, or even millions of times per day. (In fact, Amazon already updates prices an estimated 2.5 million times per day online, and there is nothing to prevent a digital price tag in a physical store from doing the same.)

Each of these AI technologies poses serious civil rights risks to consumers. To start with facial recognition technology, there is extensive evidence that facial recognition systems have varying accuracy depending on a consumer's race, gender, and age. For example, some facial recognition systems have error rates for black women that are up to 100x that of middle-aged white men. When a facial recognition system misidentifies someone, it can result in people being followed around a store, kicked out of a store, or even arrested. We are at a very real risk of our public accommodations becoming re-segregated on the basis of algorithmic bias, flaunting Title II of the Civil Rights Act, as well as provisions of the New York State Civil Rights Law. Currently, Assemblymember Tony Simone is carrying legislation that would outlaw facial recognition in places of public accommodation, A7625. Alongside bans for use by landlords, schools, and law enforcement, this bill is a part of a package put forward by a number of organizations in the Ban The Scan Coalition. You can go to banthescan.org for much more information on the dangers of facial recognition and other biometrics to consumers and all New Yorkers.

AI systems are being used in increasingly broad contexts, including housing and employment. Currently, a large percentage of applications for housing and employment are screened by AI

systems, and – like facial recognition systems – these AI algorithms tend to discriminate against women and people of color. Problems with dynamic pricing are similar, as there are no safeguards to prevent dynamic pricing to be coupled with facial recognition or other identity recognition to create personalized pricing, which is likely to charge marginalized individuals more money.

This algorithmic discrimination that consumers face, and will increasingly face to even larger extents, is particularly pernicious, because it is difficult to spot for multiple reasons. First, the AI systems making these decisions with respect to consumers are "black box," meaning that how they work and what they consider are not public. As a result, it is extremely difficult to determine whether a system's decision was made as a result of illegal bias.

Worse, even if systems are opened up to testing for bias – such as bias audits that have been proposed in several New York State bills – we do not have any standard way to test for such bias. Unlike tax audits, which – absent fraud – should come out the same way regardless of who conducts them, bias audits can be conducted in countless different ways, and can yield dramatically different results depending on methodology. As a result, there is a strong financial incentive for auditors and the AI developers that hire them to collaborate to ensure that AI systems pass these audits. Then, consumers are worse off than if the audits were not conducted, because AI developers and AI deployers can hide behind the "audit" as a defense against civil rights lawsuits.

While there is no silver bullet solution, STOP strongly recommends looking to a European model to regulate AI bias. Specifically, STOP recommends a "burden shifting" model, wherein consumers who feel that an AI system has discriminated against them illegally can sue, and there is an initial presumption at the Motion to Dismiss stage that the lawsuit is meritorious, which could only be rebutted by extensive evidence from the developer and/or deployer. Should the presumption not be rebutted, the consumer would be able to get "discovery" of the underlying algorithm – meaning that they (or their lawyers) would be able to test the algorithm for bias themselves, under a protective order to prevent trade secrets from being leaked. Then, rather than relying on a third-party auditor hired by the developer, a consumer can conduct their own audits and tests, and make their own arguments to the judge about whether the software was biased.

Barring this solution, the next best option would be to put a moratorium on most AI systems until a standardized auditing procedure is available. While such work is extremely difficult, if a regulator could create a functional, standardized auditing mechanism, the legislature could require that developers conduct such standard audits before selling or deploying their technology.

<u>False Advertising</u>

The second category of harm from AI systems to consumers is false advertising. On May 6, 2024, STOP issued its report entitled, "Selling Surveillance: Fact vs. Ad Fiction." The report reviews several types of AI surveillance systems – including computer vision, firearms detection, facial recognition, predictive policing, surveillance robots, and gunshot detection, finding that the marketing materials for each does not reflect the evidence-based reality of their capabilities.

This problem is largely true for AI systems in other contexts as well. Because systems are black-box, AI vendors are free to make outlandish claims about the effectiveness of their systems, and there is little ability for consumers to verify the claims. As a result, AI vendors are already selling snake-oil to New Yorkers.

With no way for consumers to verify these claims, it is critical that the legislature step up to create enforcement mechanisms to prevent this fraud.

Privacy

Lastly, I want to touch on privacy very briefly, because this is a subject that could last the entire hearing. As consumers interact with AI systems, their data gets harvested, aggregated, processed, and shared – usually without their consent or even knowledge. The legislature has several comprehensive data privacy bills of various strengths. Last session, the legislature passed the Child Data Privacy Act – relatively strong protections that unfortunately extend only to children and not to adults. The New York State Senate has passed a particularly weak bill – the New York Privacy Act. This bill adopts an "opt out" model of data privacy that will perpetuate the status quo – where companies take as much data as they want, secure in the knowledge that almost no one opts out. California and Europe have already adopted opt-out models, and it is clear that neither Californians nor Europeans have data privacy that is substantially improved over New Yorkers'. Passing the New York Privacy Act would further entrench this industry-supported, watered down system of data privacy that would foreclose meaningful regulation for the foreseeable future. On the other hand, passing legislation like the Digital Fairness Act, carried by Assemblymember Catalina Cruz as A3308, would be a game-changer. It would require companies to minimize data collected and require opt-in consent to collect data.

However, even if New York State passes laws requiring confidentiality of data, the cybersecurity risks of such massive commercial datasets are enormous. Just recently, the social security number of nearly every single American was compromised in a data breach. But in a worst case, a social security number can be changed. That is not the case for – say – biometric data. If this data is compromised, it is compromised for life, and biometric identification systems become identity theft risks for life.

The stakes here are enormous. Once a dataset exists, there is nothing to stop law enforcement from accessing it – usually without a warrant particularized to the individuals whose data is

being searched. For example, law enforcement can seek a "geofence warrant" to identify everyone in a given location at a given time, without needing probable cause as to the individuals searched. This can result in a geofence warrant being placed around a mosque, a protest, or an abortion clinic. Assemblymember Solages' A3306 would ban New York law enforcement from seeking such warrants. While that would be a huge step forward, it only scratches the surface of the problem, as it does not stop out-of-state law enforcement from going to their home courts and getting warrants for New Yorkers' data or for data from their residents while in New York. The implications for, say, abortion and gender-affirming care are clear.

While, again, there is no silver bullet here, Assemblymember Dinowitz' Electronic Communication Privacy Act (A1880, which has passed the Assembly but not the Senate) and Assemblymember Rosenthal's Health Data Privacy Act (A4983, which has passed the Senate but not the Assembly) would begin to create limits to law enforcement access to our private data.

Even if all this legislation passed, there would be much to do. STOP is excited to work with you all to protect consumers from the harms of the spread of artificial intelligence, while still permitting technological advancements that can improve New Yorkers' lives. If you have any questions, would like to see studies to back up this testimony, or would otherwise like to continue the discussion, please let us know. STOP is always available.

Artificial Intelligence has a rich history spanning nearly 70 years, with modern developments primarily centered around *machine learning*. These technologies produce algorithms and models that mimic intelligent behaviors learned from data. The most recent advancements in machine learning, known as *deep learning*, rely on models composed of millions or even billions of simple computational units, called *artificial neurons*, arranged in multiple layers. These models, often referred to as *deep neural networks*, have a remarkable ability to recognize and represent complex patterns in data, ranging from an individual's online browsing history to social media posts, text, images, audio, and video.

Deep learning-based AI models serve two key purposes: *analytical or predictive AI*, which analyzes data to categorize it or forecast future outcomes, and the more recent *Generative AI* technologies that creates realistic text, images, audio, and videos that are difficult to distinguish from real-world content. Since the release of OpenAI's ChatGPT in late 2022, we have witnessed the rapid acceleration of generative AI technologies. According to the 2023 State of AI Report by Stanford University[1], the U.S. generative AI industry was valued at approximately $25 billion, with projections for a compound annual growth rate of 25.6% from 2024 to 2030. Continued innovations in this field make the creation of realistic content easier and faster than ever before.

All it takes is an idea: simply describe it in a few words or sentences and input it via a user-friendly web interface. In no time, various online services can produce realistic content across multiple formats. For example, text generation is possible with tools like OpenAI's ChatGPT[2], Anthropic's Claude[3], or Google's Gemini[4]. For images, platforms such as Flux AI[5], Stable Diffusion[6],

[1] https://www.weforum.org/agenda/2024/04/stanford-university-ai-index-report/

[2] chat.openai.com

[3] anthropic.com/index/claude

[4] ai.google

[5] fluxai.com

[6] stablediffusionweb.com

MidJourney[7], X platform's Grok AI[8], Ideogram[9], and OpenAI's DALL-E[10] offer powerful generative capabilities. Audio can be synthesized with tools like Parrot AI[11] and ElevenLabs[12], while video generation services such as OpenAI's Sora[13], Runway[14], Pika[15], and Ke-ling[16] provide advanced video creation options.

However, generative AI technologies, when used maliciously, can be exploited to deceive or mislead consumers. This malicious use of AI-generated content is often referred to as *deepfakes*, combining their *deep* learning origins with their *fake* content nature.

Deepfakes introduce new risks to consumers. Some examples include:

1. Financial and privacy scams: AI-generated voice technology is being used in scams to impersonate individuals and authorize fraudulent money transfers, as well as in ransomware attacks and identity theft[17].
2. Falsified social media marketing: AI-generated videos of celebrities or influencers are used to falsely promote products or services, deceiving followers and consumers[18].
3. Online marketplace fraud: AI-generated images are used to sell counterfeit or falsified products, making it difficult for consumers to verify

[7] midjourney.com
[8] x.ai
[9] ideogram.ai
[10] openai.com/dall-e
[11] tryparrotai.com
[12] elevenlabs.io
[13] openai.com
[14] runwayml.com
[15] https://pika.art/
[16] keling.io
[17] https://www.nytimes.com/2023/08/30/business/voice-deepfakes-bank-scams.html
[18] https://www.cbsnews.com/news/taylor-swift-le-creuset-ai-generated-ads/

authenticity [19] . Large language models can generate fake reviews, misleading potential buyers and skewing online product ratings[20].

Deepfakes' harm extends beyond these. They are used to spread disinformation during political campaigns, launch discrediting attacks on individuals via social media, and target women or underage girls by creating AI-synthesized explicit images or videos of the victims, causing significant personal and emotional damage. These emerging threats highlight the urgent need for enhanced consumer protection and regulatory measures to address the misuse of generative AI technologies.

The situation calls for closer collaboration between federal and state legislatures, social platforms, media outlets, AI companies, and academic researchers[21]. To effectively combat deepfakes, we must develop technologies to detect, contain, and prevent their creation, as well as privacy protection to prevent misuse of personal data for training, and authentication methods to verify content provenance. Social platforms, online markets, and generative AI companies must actively deploy counter technologies and other guardrails, and stronger regulations should address the open-source tools and data fueling deepfake production. Increased investment in research for countermeasures is essential, along with public education to raise awareness and vigilance, especially among vulnerable and underrepresented minority groups.

[19] https://medium.com/@alex.chapman93/people-are-using-ai-to-sell-fake-items-on-etsy-b550001563fe

[20] https://www.nbcnews.com/tech/tech-news/online-product-reviews-are-becoming-battlefield-modern-ai-rcna94710

[21] https://www.techpolicy.press/deepfake-dilemma-urgent-measures-needed-to-protect-american-institutions/

Artificial Intelligence has a rich history spanning nearly 70 years, with modern developments primarily centered around *machine learning*. These technologies produce algorithms and models that mimic intelligent behaviors learned from data. The most recent advancements in machine learning, known as *deep learning*, rely on models composed of millions or even billions of simple computational units, called *artificial neurons*, arranged in multiple layers. These models, often referred to as *deep neural networks*, have a remarkable ability to recognize and represent complex patterns in data, ranging from an individual's online browsing history to social media posts, text, images, audio, and video.

Deep learning-based AI models serve two key purposes: *analytical or predictive AI*, which analyzes data to categorize it or forecast future outcomes, and the more recent *Generative AI* technologies that creates realistic text, images, audio, and videos that are difficult to distinguish from real-world content. Since the release of OpenAI's ChatGPT in late 2022, we have witnessed the rapid acceleration of generative AI technologies. According to the 2023 State of AI Report by Stanford University[1], the U.S. generative AI industry was valued at approximately $25 billion, with projections for a compound annual growth rate of 25.6% from 2024 to 2030. Continued innovations in this field make the creation of realistic content easier and faster than ever before.

All it takes is an idea: simply describe it in a few words or sentences and input it via a user-friendly web interface. In no time, various online services can produce realistic content across multiple formats. For example, text generation is possible with tools like OpenAI's ChatGPT[2], Anthropic's Claude[3], or Google's Gemini[4]. For images, platforms such as Flux AI[5], Stable Diffusion[6],

[1] https://www.weforum.org/agenda/2024/04/stanford-university-ai-index-report/

[2] chat.openai.com

[3] anthropic.com/index/claude

[4] ai.google

[5] fluxai.com

[6] stablediffusionweb.com

MidJourney[7], X platform's Grok AI[8], Ideogram[9], and OpenAI's DALL-E[10] offer powerful generative capabilities. Audio can be synthesized with tools like Parrot AI[11] and ElevenLabs[12], while video generation services such as OpenAI's Sora[13], Runway[14], Pika[15], and Ke-ling[16] provide advanced video creation options.

However, generative AI technologies, when used maliciously, can be exploited to deceive or mislead consumers. This malicious use of AI-generated content is often referred to as *deepfakes*, combining their *deep* learning origins with their *fake* content nature.

Deepfakes introduce new risks to consumers. Some examples include:

1. Financial and privacy scams: AI-generated voice technology is being used in scams to impersonate individuals and authorize fraudulent money transfers, as well as in ransomware attacks and identity theft[17].
2. Falsified social media marketing: AI-generated videos of celebrities or influencers are used to falsely promote products or services, deceiving followers and consumers[18].
3. Online marketplace fraud: AI-generated images are used to sell counterfeit or falsified products, making it difficult for consumers to verify

[7] midjourney.com
[8] x.ai
[9] ideogram.ai
[10] openai.com/dall-e
[11] tryparrotai.com
[12] elevenlabs.io
[13] openai.com
[14] runwayml.com
[15] https://pika.art/
[16] keling.io
[17] https://www.nytimes.com/2023/08/30/business/voice-deepfakes-bank-scams.html
[18] https://www.cbsnews.com/news/taylor-swift-le-creuset-ai-generated-ads/

authenticity [19] . Large language models can generate fake reviews, misleading potential buyers and skewing online product ratings[20].

Deepfakes' harm extends beyond these. They are used to spread disinformation during political campaigns, launch discrediting attacks on individuals via social media, and target women or underage girls by creating AI-synthesized explicit images or videos of the victims, causing significant personal and emotional damage. These emerging threats highlight the urgent need for enhanced consumer protection and regulatory measures to address the misuse of generative AI technologies.

The situation calls for closer collaboration between federal and state legislatures, social platforms, media outlets, AI companies, and academic researchers[21]. To effectively combat deepfakes, we must develop technologies to detect, contain, and prevent their creation, as well as privacy protection to prevent misuse of personal data for training, and authentication methods to verify content provenance. Social platforms, online markets, and generative AI companies must actively deploy counter technologies and other guardrails, and stronger regulations should address the open-source tools and data fueling deepfake production. Increased investment in research for countermeasures is essential, along with public education to raise awareness and vigilance, especially among vulnerable and underrepresented minority groups.

[19] https://medium.com/@alex.chapman93/people-are-using-ai-to-sell-fake-items-on-etsy-b550001563fe

[20] https://www.nbcnews.com/tech/tech-news/online-product-reviews-are-becoming-battlefield-modern-ai-rcna94710

[21] https://www.techpolicy.press/deepfake-dilemma-urgent-measures-needed-to-protect-american-institutions/

Testimony of the New York News Publishers Association

Assembly Committee on Consumer Protection

Assembly Committee on Science and Technology

September 20, 2024

Introduction

Thank you for the opportunity to testify on behalf of the New York News Publishers Association. NYNPA represents 60 print and digital newspapers, including some which have been publishing for 200 years, and some for two years. We represent news organizations with global audiences, small local not-for-profit newspapers, and a variety of sizes and ownership structures.

Our members employ thousands of professional journalists who provide their communities with factual, curated news about their local governments and the lives of their neighbors. Journalists provide more than a simple recitation of facts. They use professional judgment to determine the meaning of facts, placing them in context, compiling and explaining information they gather in ways that will be meaningful to readers. The presence of journalists in a community helps instill trust and familiarity with members of the community, which in turn improves news coverage.

Our ability to cover our communities has been deeply eroded over the past 15 years and is now facing an extinction level threat with the advent of generative artificial intelligence.

Advertising traditionally provided about 85% of a newspaper's revenue when most advertising appeared on the pages of a printed newspaper.

Digital advertising has always been comparatively cheap and has never replaced print ad revenue. Over the years, Google acquired companies such as Double-Click, amassing control over the sale, display and placement of digital advertising, leaving news websites with only a very small share of the revenue. Google's search function has displayed portions of newspaper stories to attract readers and the advertisers who seek reader attention, although only a relatively small percentage of internet visitors ever click through to the newspaper's website.

Overall newspaper revenues have declined by more than half over the past few years.

Thousands of newspapers throughout the country have closed. Others have consolidated to save money, sold off their presses and buildings, and drastically cut staff.

Things are about to get worse.

Tech companies' chat services compete with news organizations by engaging in wholesale copying of news content to train Large Language Models fueling services which provide a reader with a summary in answer to a query rather than a link to a news website. These companies copy news content, even when the newspaper company clearly prohibits it - even scraping content from behind newspaper paywalls. LLMs train chat services to mimic the style, tone and manner

of news reporting by human journalists in order to engage the attention of readers, which in turn attracts advertisers.

This is a threat not only to news organizations with global reach, but also to smaller community newspapers. One of our members, The Columbia Paper, reported on the election of the first Black mayor in the City of Hudson. Publisher Warren Dews decided to see if the news had popped up on the internet. He found a detailed story on a chat service about the new mayor, which was a very close replication of his newspaper's story.

GAI-created summaries mix carefully curated journalism with random scrapings from all corners of the internet. As a result, readers are sometimes provided with inaccurate information. A photojournalist acquaintance reported searching for his name on Chat GPT, which accurately listed his career highlights and many awards, as well as his untimely death from cancer, to his surprise.

Because chat services present a mix of accurate content produced by news organizations with random misinformation, news organizations' reputations can be harmed by association with misinformation.

As news organizations' revenues and reputations are eroded, many will be forced to close, depriving the internet of reliable sources of information, and it will rot from the inside out.

The decline in local news poses harm to New York State residents. Research shows that the existence of a local newspaper is directly correlated with lower costs of municipal financing (2018 Hutchins Center working paper), with higher civic engagement (Journal of Politics, 2017) and a lower level of extreme partisanship (Journal of Communication, 2018).

How Can Newspapers Be Preserved?

New York State government recognized the plight of newspapers by enacting the Newspaper and Broadcast Jobs Tax Credit this spring. This three-year program set to begin in January 2025 will help preserve many journalism jobs while structural changes in the news ecosystem are put into place.

News organizations and others have sued companies which misappropriate and misuse their content (Case Tracker: Artificial Intelligence, Copyrights and Class Actions | BakerHostetler (bakerlaw.com). But the litigation is complex and will take years to work its way through the courts.

GAI can provide significant benefits to society, but only if one of the most important sources of quality data – news organizations – can survive and participate voluntarily and fairly with adequate compensation for the use of their products. Professionally gathered journalism has value, and there is a long history of news content being licensed for use by non-news purposes.

Transparency and accountability in the use of news content is also vital. Consumers should be presented with detailed information about the sources of GAI generated content, and news organizations should be notified when their content is accessed for possible re-publication, for any purpose, by any entity, or when GAI developers use publishers' valuable, high-quality

writing to add value to their own products in training their large language models.

The News Media Alliance, which represents newspapers, magazines and digital media on a national level, has published a detailed white paper suggesting solutions, many of which must be accomplished through federal legislation or regulation in order to avoid preemption by federal copyright law (White Paper: How the Pervasive Copying of Expressive Works to Train and Fuel Generative Artificial Intelligence Systems Is Copyright Infringement And Not a Fair Use (newsmediaalliance.org)).

We would be pleased to discuss potential state-level actions with the Legislature, Governor Hochul and Attorney General James.

Statement of

David L. Donovan

President

New York State Broadcasters Association, Inc.

before the

New York State Assembly

Standing Committee on Consumer Affairs and Protection

and

Standing Committee on Science and Technology

September 20, 2024

Good morning, Chair Rozic and Chair Otis, as well as members of the committees on Consumer Affairs and Protection and Science and Technology. My name is David Donovan, and I am president of the New York State Broadcasters Association. NYSBA is a non-profit trade association representing more than 400 local radio and TV broadcast stations that are licensed by the FCC to serve communities throughout the Empire State.

Local radio and television stations are essential to provide unbiased ***local*** news and information to their communities. Unlike national cable news channels, our focus is local. Local stations are the place where citizens learn about weather conditions, school closings, traffic congestion, sports, police actions and most importantly, local government activity. While local stations are retransmitted by cable systems, satellite services, and digital platforms, consumers can receive our signals and local news for free by using an inexpensive antenna. We provide a universal platform that serves all New Yorkers, rich and poor, urban and rural. In addition, while local stations may be "affiliated" with major broadcast networks, most local stations in New York State are licensed to other companies. The local stations owned by the major networks in New York City are focused on meeting the needs of the many diverse communities in the city.

At the outset, it is worth noting that nearly all the misinformation being spread by the deceptive use of "AI" appears on digital and social media platforms. Simply stated, local broadcasters are not the primary problem. Nonetheless, we recognize that New York wants to protect its citizens from the unscrupulous use of "AI." In doing so, we would ask that you consider the unique challenges facing local broadcasters in today's hypercompetitive media marketplace. In this regard, we want to thank Chairman Otis for sponsoring recent legislation that helped correct a number of issues regarding "AI" in the context of political communications.

"AI" is a tool and, if used properly, can help broadcasters better serve their local communities. A station can use it to help manage its own content. "AI" can provide an efficient tool for research and analytics. It can help reporters and newsrooms create accurate news content more efficiently. We ask that you consider the following issues as you move forward with legislation.

First, over the past few years, local broadcasters have experienced big tech companies "scraping" our content, repackaging it, and using that content for their own digital platforms to compete for advertising against local stations. The noted communications economics firm BIA Kelsey found that local stations have lost $1.873 billion in value due to this practice. Developers of generative artificial intelligence systems are using local content to help train their "bots." Eight U.S. Senators recently wrote to the FTC asking it to investigate whether these practices violate federal law.[1] If local broadcast journalism is to remain viable, then legislation is necessary to prevent content "scraping." Moreover, policy must be directed towards providing fair compensation for local stations in New York.

Apart from economic loss, "AI" scraping of local broadcast news content may have significant negative effects on the communities we serve. New Yorkers rely on their local radio and television stations as a trusted news source. Today, an unscrupulous entity can use "AI" to distort our news programming, distribute it on a digital platform, and contribute to misinformation in communities throughout New York. To preserve the integrity of local news, we believe New York should explore ways to address this problem.

[1] Letter to the Honorable Jonathan Kanter, Asst. Atty General, Antitrust Division, Department of Justice and the Honorable Lina Kahn, Chair, Federal Trade Commission from Sen. Amy Klobuchar, Sen. Richard Blumenthal, Sen Mazie Hirono, Sen. Richard Durbin, Senator Sheldon Whitehouse, Sen. Tammy Duckworth, Sen Elizabeth Warren and Sen. Tina Smith, September 10, 2024. https://www.klobuchar.senate.gov/public/_cache/files/2/8/28792e8d-9f57-4f82-84eb-810103e85084/2E67A60C5FD8132EB31EBCDFD9DFF9078BEDD557974D621951B43B0597175096.final-letter-to-doj-ftc---competition-issues-with-generative-ai-and-content---9.10.24.pdf

Second, liability for using deceptive "AI" must rest on the entity that ***creates*** the content. This would apply to advertising and other programming. The content creator is in the best position to know and should bear the responsibility to ensure that "AI" is used properly.

Stations accept legal responsibility for what is broadcast on their stations, but "AI" presents a unique challenge. The fundamental problem is that stations do not know if content received from third parties contains "AI." Technology that can detect "AI" content has become involved in an arms race, as technology to counter detection methods is being developed at an equal pace.

In the context of news, the issue is whether imposing liability will "chill" news coverage. Such an unintended result could have significant First Amendment implications. The newsrooms at local stations are bound by journalistic standards with respect to content that is included in the newscast. Our business depends on maintaining public trust. If errors are made, they are corrected. As noted previously, local broadcast news is not the problem.

With respect to local advertising, stations often receive content produced by advertisers and advertising agencies. Again, it is impossible to discern if deceptive "AI" has been included, given the growing quality of "AI" voices and images. The responsibility should rest with the creator of the advertising.

Local stations broadcast a significant amount of nationally distributed news and entertainment programs. Local stations do not create this content. Moreover, local stations have a contractual obligation to broadcast these programs, including any national or regional advertising contained within the programs. Radio and television stations receive hundreds of programs and thousands of advertisements per week. Content is distributed by satellite or fiber and received by a station in "real" or "near real" time. While local stations do their best, it is

extremely difficult, if not impossible, to "prescreen" all programs and advertising before they are aired.

Again, "AI" liability policies should be directed towards those who ***create*** the content and not a local broadcaster transmitting the program. To avoid chilling speech, legislation should include an exemption for local stations, especially news operations. Local stations that create the content should be responsible where they have **actual knowledge** that the content used in the creation of the content contains manipulative or deceptive "AI." This standard is consistent with the First Amendment.

Third, we would like you to consider the potential negative impact on a local station's advertising revenue from certain labeling requirements often used in "AI" legislation as a means to inform consumers. Broadcasters generally have no problems with labels *per se*. We use them all the time to comply with state and federal regulations. Special consideration, however, must be given to the uniqueness of radio broadcasting. A typical radio advertisement is 30 seconds, and 15 second spots are not uncommon. Requiring lengthy labels renders radio advertising useless, resulting in advertisers shifting to digital platforms. Advertising is the sole primary source of revenue for radio stations, and the loss of this revenue undermines a station's ability to serve its local community.

Fourth, any legislation must also consider the impact of federal law. For example, mandating labels may conflict with federal law as applied to political advertising provided by a candidates authorized campaign committee. In addition, federal activity may result in the application of both state and federal labels for the same content. Finally, requiring specific labels on content, especially news content, may constitute compelled speech and violate the First Amendment.

Finally, our concerns about "scraping" our content and establishing rules that drive away advertising revenue raises an overarching policy question. The economics of providing local broadcast journalism are challenging and stations depend on advertising as a primary source of revenue. Driving advertisers away from broadcasting and on to digital platforms undermines our ability to serve our communities. Moreover, such policies directed at local stations may miss the mark because the real problem with misinformation from "AI" rests primarily on digital platforms and user generated content not associated with local broadcasters.

From a broadcaster's perspective, "AI" is a significant new tool that can help us serve our communities. We look forward to working with the committees to help craft legislation that protects consumers and ensures the continued provision of local news and information to Communities throughout New York.

Respectfully submitted,

David L. Donovan
President
New York State Broadcasters Association, Inc.
1805 Western Avenue
Albany, NY 12203
(518) 456-8888
ddonovan@nysbroadcasters.org

REBECCA DAMON

TESTIMONY ON BEHALF OF
THE SCREEN ACTORS GUILD - AMERICAN FEDERATION
OF TELEVISION AND RADIO ARTISTS

TO THE

ASSEMBLY STANDING COMMITTEE ON CONSUMER
AFFAIRS AND PROTECTION
ASSEMBLY STANDING COMMITTEE ON SCIENCE AND TECHNOLOGY

SEPTEMBER 20, 2024

Good morning, Chair Rozic, Chair Otis, and distinguished members of the Assembly. I am Rebecca Damon, Chief Labor Policy Officer and New York Local Executive Director at Screen Actors Guild – American Federation of Television and Radio Artists ("SAG-AFTRA"). Thank you for this opportunity to comment on the importance of ensuring consumer protection and safety relating to the use of artificial intelligence ("AI"). This is a topic of critical – even existential – importance to SAG-AFTRA and its members, and we appreciate the committees' attention to it.

SAG-AFTRA is the nation's largest labor union representing entertainment and media artists. Its membership includes over 160,000 actors, news and entertainment broadcasters, recording artists, and other entertainment professionals (collectively "artists"). Hundreds of thousands of individuals have worked under our contracts, including many who have served in the government – even in the White House.

I speak today to highlight the importance of regulating artificial intelligence to protect against non-consensual replication of voice and likeness, and the importance of regulating against the dangers AI presents more broadly. AI technology poses an existential threat to creative workers, and we are seeing increasing dangers to consumers, civil discourse, student health and welfare, democracy and national security.

Last year, SAG-AFTRA reached a historic agreement with the major entertainment studios which included, among other important provisions, the first comprehensive terms governing the use of artificial intelligence to replicate voice and likeness in filmed entertainment projects. This agreement followed the longest entertainment industry strike for our TV/Theatrical and Streaming contract in over forty years, a strike that lasted nearly four months. Subsequently, we successfully concluded similar negotiations with the major record labels, including the first comprehensive terms related to AI in the music industry. Unfortunately, we are now on strike against major video game producers who refuse to recognize the protections our members need in this age of generative AI.

The 2023 strikes – and the public's response to them – highlighted the importance of AI, both to the entertainment industry and the broader public. AI technology is making it exponentially easier, cheaper, and faster to create convincing, realistic digital replicas of individuals, and to create synthetic creative content that displaces the work of human creators. New York has positioned itself at the forefront of this fight over sensible AI protections. New York recently enacted a law to protect individuals from exploitation in nonconsensual, sexually explicit deepfakes, and we continued to build out protections from exploitation by replication for deceased performers. SAG-AFTRA championed the 2024 passage of legislation requiring

informed consent and proper representation when licensing digital replicas to replace human work, and we look forward to Governor Hochul signing that bill soon.

Scammers, using AI technology, have aggressively taken to social media with AI-generated versions of beloved celebrities to defraud consumers. AI versions of Tom Hanks, Taylor Swift, Selena Gomez and many other celebrities have all been used in social media-based scams that, collectively, reached millions of US and European users, according to one report. In most of these scams, the fraudulent ads link to sites that resemble official corporate sites where victims are further tricked into spending money and signing up for expensive subscriptions that are difficult to cancel. In addition, lesser-known content creators or "influencers" have been exploited. A "Christian social media influencer who posts about travel, home decor and wedding planning" had her most popular video turned into an ad for erectile dysfunction using an A.I.-generated voice. And a 20-year-old college student at the University of Pennsylvania, who is of Ukrainian descent, found an A.I.-generated version of herself spewing pro-Russia propaganda in Mandarin, a language she does not speak. We are all engaging online today, and the digital marketplace is unfortunately ripe for abuse by bad actors using A.I. if we do not act.

These scams victimize not only the consumer, and the professional and reputational harm to the depicted individual; they also harm the legitimate companies with whom the depicted individual has a professional relationship, and they erode confidence in commerce and commercial transactions. There should be disclaimers for AI generated digital replicas, protections against non-consensual uses, there should be standards to track and source AI generated material, and there should be repercussions for making AI systems openly available without proper safety protocols. If a consumer is engaging with a synthetic AI-created voice or likeness, say a chatbot or avatar assistant or salesperson, they should, at minimum, know that it is

AI. SAG-AFTRA supports Assemblymember Rosenthal and Senator Gianaris's legislation, A.216-C/S.6859-A, which requires that "synthetic performers" in commercial advertising, in any medium, are always accompanied by a clear and conspicuous disclaimer. We look forward to advocating for this bill in 2025, which is another piece in the puzzle to protect consumers and workers alongside the advancement of this technology.

Our industry has shown that it is critical this space be regulated, and we have shown that it can be done in a thoughtful manner. We are not here to ban artificial intelligence – AI promises to deliver unparalleled progress in many areas of life. However, we are here to protect human creative endeavors and the jobs they provide. We are here to ensure that AI does not erode confidence in the legitimate human-created entertainment world by an avalanche of fakes. And we are here to protect the public's trust in media. SAG-AFTRA looks forward to working with you all in 2025 and beyond on smart, worker-centered AI policy.

I thank the members of the Committee for this opportunity to speak, and I look forward to answering any questions you may have.

Tech:NYC 9/20 Assembly Hearing Testimony

Good morning, I'm Marjorie Velazquez. I'm Vice President of Policy at Tech:NYC, a nonprofit member-based organization representing over 800 technology companies in New York.

Overview: Businesses are using AI to help with increasing efficiency and expanding their services without expanding their costs.

This includes everything from low-cost AI-enabled services that help small businesses reach their customers, and tools that allow hospitals to interpret data for medical research, to companies such as OpenAI, Google, IBM, Salesforce, Deloitte, and Accenture that offer AI products for data analytics and creating business efficiency at scale.

And these technologies are growing our economy — since 2019, 1,000+ AI-related companies in NYC have raised $27B in funding and there are more than 40,000 AI professionals in NYC alone.

AI technologies are being rolled out all over the world. It's crucial that New York State works to ensure they are developed here. This is why we have supported Empire AI, a first-in-the-nation effort to ensure our research institutions have access to best-in-class technical resources to help find solutions to all sorts of challenges — from climate to health care and beyond.

AI Regulations & Proposals in NY: New York City was an early mover when it comes to AI regulation. In 2021, the City Council passed local law 144, which requires disclosures of and bias audits for AI tools used in hiring processes.

AI tools are crucial to supporting hiring processes when roles can see hundreds or thousands of applicants — and even more when organizations do not have the resources or staff dedicated to hiring.

A similar proposal also exists today in the state legislature (A9315/S762).

Tech:NYC recommends that the state legislature pass a bill that is as similar as possible to NYC's Local Law 144, for two main reasons:

One, companies hiring across both New York City and New York State should not have to face different compliance requirements when hiring candidates.

Two, the bias audits required by NYC's law created an entirely new category of assessments by accounting firms — these are still relatively new, and must be analyzed before more laws expand their usage.

Looking ahead, it's clear that there will be legislation for AI tools that impact significant life decisions.

Recommendations for AI Regulation: To make sure that future regulations are not an additional administrative burden, **Tech:NYC recommends that proposals in New York adopt a risk-based approach.**

The reality is that countless businesses use AI in ways that either do not directly impact consumers or that actively benefit everyday New Yorkers. A risk-based approach varies levels of regulation based on the risk level of decisions involving AI.

This reflects the EU's AI regulations. Tiered AI regulation — and the disclosures required — reserves the most oversight for

- Products that could lead to harmful results or
- AI that impacts integral life decisions such as healthcare, financial resources, housing, and more.

Additionally, to make sure AI technologies are not the decision-makers, **all main decision points can require human review of varying levels.**

The more sensitive decisions should require higher levels of human review, and review requirements should be focused at decision points that actually impact a consumer.

This would address concerns raised by the NYS LOADinG Act (S7543/A9430), which regulates AI used by government agencies by requiring "continued and operational meaningful human review". That level of review is inefficient and vague.

Layers of Responsibility: As we consider the private sector's use of AI tools, we need to examine how to assign responsibility to the parties involved in the development of AI tools and determine the necessary regulations to address this.

Consider a business that trains an AI chatbot based on its own company information. AI tools are developed by a cloud-based provider that creates both the program and training data, which is then further altered and trained by secondary developers, and then ultimately tailored by an end user for maximum impact.

The end user must not be held responsible for compliance of technologies they have not developed.

This reflects Article 53 of EU's AI Act, which requires Providers of General-Purpose AI Models to provide technical documentation of their models, including their training and testing process, and evaluations.

Generative AI Labeling and Disclosures: The FY25 NYS Budget included new regulations on content created with AI, ensuring protections for the public when this content could be used for misinformation or deception, or to create sexually explicit content.

To address and go beyond these instances, Content Provenance and Authentication Standards have been developed by industry stakeholders. These offer credentials, or tags, that track metadata and can be added to content to let users know if images or videos have been created or altered using AI.

It is crucial for the government to support these credentials, and **Tech:NYC has two recommendations:**

- First, state agencies should require these credentials on any content produced or published by New York State.
- Second, online platforms should be required to maintain any authenticity credentials or tags when content is uploaded by users or third parties to these platforms.

Clarity is Key: One way to address AI concerns is through piecemeal legislation. Another is to establish an overarching strategy on tools that impact consumers. Tech:NYC recommends the latter, which is also a reason we would prefer federal legislation that will lead to streamlined compliance.

The development of this technology is now integral to the success of our local economy,

To continue this progress, companies and technology developers need clarity on new regulations, to whom they apply, and how they must be implemented. This is imperative for companies and organizations to continue to develop their impactful technologies to benefit businesses and everyday New Yorkers.

Thank you.

Good morning,

My name is Hayley Tsukayama, speaking today on behalf of the Electronic Frontier Foundation. EFF, founded in 1990, is a San Francisco-based, non-profit organization that works to protect civil liberties in the digital age. EFF represents more than 35,000 active donors and members, including thousands of supporters in New York.

We thank you for extending the invitation to speak today.

EFF advocates for individuals, which includes consumers, developers and creators. Our advocacy balances several interests such as privacy, innovation, and free expression. Artificial intelligence, AI, has implications for many of our digital liberties issues.

People can use AI to create tools with extraordinary potential. They can help users distill large volumes of information, manage numerous tasks more efficiently, and change how we work – for good and for ill, depending on where you sit. However, AI tools can also exacerbate existing bias, and move at a speed and scale that can quickly outpace oversight mechanisms.

When it comes to ensuring safety and protections, we have several suggestions for policymakers to consider.

First, **regulate uses, not technology**. AI can have many uses, not all of them are harmful. And, in cases where there is harm to, for example, privacy, that harm extends beyond the mere use of AI tools and lawmakers should address these larger issues.

Like many new technologies, AI is best understood as a tool. For this reason, EFF believes the *technology* itself is not the appropriate target for regulation. Yes, developers should make sure that their tools are developed responsibly and for the purposes they intend. But just as the maker of a kitchen knife cannot certify that their tool cannot be used to harm someone, a developer cannot guarantee their model won't be misused.

EFF opposes proposals such as California's SB 1047, that put blanket limits on computing power, the amount of hardware that can be utilized, or amount of investment. These limits not only runs the risk of freezing innovation, but also will not address root problems such as unfair decisions for mortgage applications, or biased health risk assessments.
To avoid these outcomes, we encourage lawmakers to think about the ways AI tools are used and then craft appropriate legislation to address those particular scenarios. We also encourage lawmakers to consider how existing laws can apply to AI, or how they can be amended to do so.

Second, we encourage lawmakers to **rely on data privacy principles** of transparency, notice and consent to make sure that people understand what information is being used, why, and also how it might be shared. AI tools may use data differently than other tools,

but they still rely on personal information to function. Legislation should use the expectations of consumers, not businesses, to determine which entities or purposes should be covered by laws. EFF has seen several problematic proposals, for example, that allow businesses to skirt notice requirements if the *business itself* determines that AI is not, for example, a "substantial" factor in decisionmaking. But it should not be up to businesses to decide if a law applies to them or not.

EFF has supported these principles in consumer privacy legislation across the country, as well as in AI legislation. In New York, we supported the BOT Act [S7623B
9 Hoylman-Siegal/ A9315A Alvarez], which establishes strong data privacy protections as the foundation of strong AI protections in the workplace.

As with bills addressing AI in the workplace, consumer AI bills should not center solely on transparency and auditing. They should also empower individuals to address issues on their own, with meaningful enforcement mechanisms. EFF strongly favors a private right of action to ensure that laws have the teeth to incentivize companies to place individual safety, autonomy, and privacy at the center of their goals.

And while transparency and auditing are key, to address these issues fairly, there must be places in the process available to incorporate the concerns of those subject to these algorithms and automated decision-making systems—such as appeal mechanisms. There must also be mechanisms to ensure that these conversations are taken seriously to counteract bias.

Third, **make sure any discrimination provisions in AI bills don't lower the bar** of existing protections. Many companies use AI tools to evaluate, for example, financial stability when deciding rental applications. The housing sector already has protections in place to ensure that landlords are fair, or face repercussions for unfair decisions.

AI should not be an excuse for discrimination. Proposals should be carefully crafted to ensure against, for example, creating a definition of "algorithmic discrimination" that is less stringent than existing law.

Finally, remember that **government can and should set a high bar** by putting in strong transparency, privacy, pre-deployment evaluation, and audit requirements for their own AI procurement for state and local agencies. While government use of AI is not the subject of today's discussion, EFF notes that we have seen several bills that intend to curb harmful practices by private companies but create exemptions for government contractors or partners—essentially giving some private companies a pass. Yet private companies working on behalf of the government often handle highly sensitive data from vulnerable populations and should be held to the same, if not stricter, standards because of it.