Report of the Generative AI and Natural Language Processing Task Force

December 2024

Letter from the Co-Chairs

On behalf of the Generative AI and Natural Language Processing Task Force, we are pleased to submit this report to the Governor and Illinois General Assembly. Over the past six months, our bipartisan and multi-sectoral task force has undertaken a thorough examination of the evolving Generative AI landscape. Guided by Public Act 103-0451, our charge has been to explore the opportunities, risks, and implications of these technologies for our state and its residents.

Generative AI technologies are advancing rapidly, raising both opportunities and significant challenges. As a task force, our priority has been to provide a clear-eyed assessment of these developments and their implications for Illinois. This includes identifying pathways to responsibly harness the benefits of these technologies while addressing the very real risks they pose to privacy, equity, and public trust.

The recommendations in this report reflect a commitment to protecting the public interest and ensuring that Generative AI is deployed in ways that serve our communities fairly and ethically. Illinois has an opportunity to lead in this space by fostering innovation that is balanced with strong safeguards for individuals and families. By centering transparency, accountability, and equity, we can meet these challenges head-on.

This report is an important first step toward a holistic approach to generative AI governance in Illinois. However, the work does not end here. There will be a continuous need to monitor and regulate the evolving AI and generative AI landscape, adapting as these technologies advance. This will require ongoing collaboration with partners in the public and private sectors, as well as with academic institutions, to ensure Illinois remains both proactive and resilient in addressing these challenges.

We are grateful for the insights and dedication of task force members, expert witnesses, stakeholders, and the public throughout this process, and to Public Citizen for their input and support. Your contributions have been essential to this effort. As we submit this report, we reaffirm our commitment to building a future where technology policy is aligned with the needs and values of the people of Illinois.

Thank you,

Co-Chairs of the Generative AI and Natural Language Processing Task Force

Representative Abdelnasser Rashid
Senator Robert Peters

Task Force Members

Angie Aramayo
Cloud Sourcing Lead, IBM

Dave Beck
Regional Director, AFSCME Council 31

Jason Bowen
Statewide Chief Information Security Officer, Illinois Department of Innovation and Technology

Jen Crichlow
Vice President of Operations, SAVVI AI

Tyler Diers
Executive Director, Midwest, TechNet

Joseph Fatheree
Educator, Illinois State Teacher of the Year (2007)

Jerry Follis
Senior Director for Information Technology, Illinois Community College Board

Raúl Gastón
Principal, Gompers Junior High School, Joliet Public Schools District 86

Jill Gebke
Assistant Director of Academic Affairs, Illinois Board of Higher Education

Sanjay Gupta
Secretary, Illinois Department of Innovation and Technology

Jason Helfer
Chief Education Officer - Instruction, Illinois State Board of Education

Mechie Nkengla
CEO and Chief Data Strategist, Data Products LLC

Sen. Robert Peters
Task Force Co-chair

Alicia Ponce
Founder & Principal
AP Monarch

Rep. Abdelnasser Rashid
Task Force Co-chair

Deidre Ripka
Director of Secondary Education, McLean County Unit 5

Omar Salem
Educator, Niles North High School

Richard Shavzin
Executive Board Member, Illinois AFL-CIO

Sen. Win Stroller
State Senator

Matthew Van Hise
Chief Privacy Officer
Illinois Attorney General's Office

Juan M. Vasquez
Managing Director & Senior Information Security Officer, Global Cybersecurity - State Street Corporation

Dmitry Zhdanov
State Farm Endowed Chair in Cybersecurity, Illinois State University

Table of Contents

Overview

Generative Artificial intelligence (GenAI) is an increasingly influential technology that is already reshaping many aspects of society. When applied responsibly, it can provide solutions to complex challenges, enhance productivity, and foster innovation across fields. At the same time, the misuse or unregulated deployment of GenAI poses serious risks. It could amplify issues such as bias, fraud, and misinformation, disrupt labor markets by displacing workers, and worsen the climate crisis. These risks underscore the importance of developing and applying GenAI with care and foresight.

Addressing these challenges requires a collective effort involving governments, businesses, academia, and civil society. Establishing robust ethical standards, governance frameworks, and accountability mechanisms will be critical in managing GenAI's impact. Such efforts are essential to balance innovation with proper safeguards, ensuring that GenAI's benefits are realized, while minimizing its harms.

Ultimately, the goal should be to create an environment where Illinois is at the forefront of harnessing the economic power of GenAI in a socially responsible and sustainable way. GenAI is expected to grow exponentially, and like electricity and the internal combustion engine, its effects will likely be long lasting and not always easily predictable. By proactively addressing the risks and fostering a shared understanding of GenAI's potential, Illinois can better navigate this pivotal moment and maximize the benefits of GenAI for all communities in our state.

It is against this backdrop that the Illinois enacted legislation creating the Generative AI and Natural Language Processing Task Force (20 ILCS 1370/1-80), with the purpose of investigating the opportunities and challenges associated with GenAI and natural language processing (NLP) technologies. Tasked with examining their implications across multiple critical domains, the task force serves as a forum to address effects these technologies will have on Illinois residents and institutions.

Composed of educators, cybersecurity experts, AI specialists, business leaders, and public officials, the task force hosted five public meetings in hybrid formats. These sessions featured expert panelists and discussions held in Chicago, Springfield, the Metro East region, the Quad Cities, and Southern Illinois. Topics covered included consumer protection, the use of generative AI in classrooms, leveraging AI to improve public services, safeguarding civil liberties, addressing workforce and environmental implications, and strengthening cybersecurity.

Through these sessions, as well as the work of several working groups, the task force has explored both the current and future impacts of GenAI across numerous domains.

This report presents the key findings from these discussions and offers recommendations for policymaker consideration. The recommendations focus on the following domains:

- Labor & Workforce
- Civil Rights and Civil Liberties
- Consumer Protection
- Environment
- Higher Education
- P-12 Education
- Cybersecurity
- Delivery of Public Services

By addressing these areas, the Illinois Generative AI and Natural Language Processing Task Force aims to provide thoughtful guidance to ensure that the integration of GenAI benefits all Illinois residents while safeguarding their rights and well-being.

Working Groups

To effectively address the multifaceted implications of GenAI, the task force established four specialized working groups: K-12 Education, Higher Education, Labor and Commerce, and Cybersecurity.

In addition to the working groups, other key subjects were addressed through the general task force meetings. These sessions featured panel discussions with subject-matter experts, providing valuable insights on topics such as consumer protection, civil rights and liberties, the environment, and other issues. These discussions enriched the broader scope of the task force's work and informed the policy recommendations included in this report.

K-12 Education Working Group

This group focused on the responsible integration of GenAI into K-12 classrooms, addressing issues such as ethical use, equitable access, and teacher training.

- Joseph Fatheree: Illinois State Teacher of the Year (2007)
- Jason Helfer: Chief Education Officer - Instruction, Illinois State Board of Education
- Deidre Ripka: Director of Secondary Education, McLean County Unit 5

Higher Education Working Group

This group explored the use of GenAI to enhance teaching, learning, and administrative operations in colleges and universities.

- Jerry Follis: Senior Director for Information Technology, Illinois Community College Board
- Jill Gebke: Assistant Director of Academic Affairs, Illinois Board of Higher Education

Labor and Commerce Working Group

This group examined the impact of GenAI on the workforce, including job displacement, new employment opportunities, and workforce training.

- Richard Shavzin: Executive Board Member, Illinois AFL-CIO
- Jen Crichlow: Vice President of Operations, SAVVI AI
- Angie Aramayo: Cloud Sourcing Lead, IBM
- Tyler Diers: Executive Director, Midwest, TechNet
- Dave Beck: Regional Director, AFSCME Council 31

Cybersecurity Working Group

This group addressed the critical challenges GenAI poses to cybersecurity, focusing on protecting data and systems from emerging threats.

- Dmitry Zhdanov: State Farm Endowed Chair in Cybersecurity, Illinois State University
- Jason Bowen: Statewide Chief Information Security Officer, Illinois Department of Innovation and Technology
- Juan M. Vasquez: Managing Director & Senior Information Security Officer, Global Cybersecurity - State Street Corporation
- Sanjay Gupta: Secretary, Illinois Department of Innovation and Technology

Their collective expertise ensured a comprehensive evaluation of the implications of GenAI across key sectors, contributing to actionable policy guidance for the state of Illinois.

Expert Panelists

The Illinois Generative AI and Natural Language Processing Task Force benefited from the insights and expertise of a diverse group of panelists. These subject-matter experts, drawn from academia, government, advocacy organizations, and industry, contributed to the task force's understanding of the implications of generative AI and NLP across a range of domains. Their expertise informed the task force's deliberations and strengthened the policy recommendations outlined in this report.

Over the course of five meetings, the task force engaged with the following panelists:

First Meeting: June 4th, 2024

- Suresh Venkatasubramanian: Director, Center for Tech Responsibility, Brown University
- Robert Weissman: Co-President, Public Citizen

Second Meeting: August 12th, 2024

- Dr. Dorith Johnson: Assistant Superintendent of Curriculum, Instruction, Assessments, and Grants, Bloom Township High School District 206
- Dr. Tricia Bertram Gallant: Director of the Academic Integrity Office, University of California, San Diego (UCSD)
- Dr. Sepehr Vakil: Professor, Northwestern University
- Illinois State Representative Janet Yang Rohr

Third Meeting: September 18th, 2024

- Dr. Dmitry Zhdanov: State Farm Endowed Chair in Cybersecurity, School of Information Technology, Illinois State University
- Jason Bowen: Statewide Chief Information Security Officer, Illinois Department of Innovation and Technology

Fourth Meeting: October 16th, 2024

- Mike Horrigan: President, W.E. Upjohn Institute for Employment Research
- Richard Shavzin: Executive Board Member, Illinois AFL-CIO

Fifth Meeting: November 15th, 2024

- Stephen Ragan: Policy and Advocacy Strategist: Privacy, Technology, and Surveillance, American Civil Liberties Union (ACLU)
- Peter Hanna: Legal Advisor, American Civil Liberties Union (ACLU)
- Samira Hanessian: Energy Policy Director, Illinois Environmental Council
- Iyana Simba: City Programs Director, Illinois Environmental Council

The insights provided by these panelists enhanced the discussions during the task force meetings, supplying valuable information and guidance that aided members in developing the report's findings and recommendations.

In addition to the expert panel discussions, the task force actively sought and took into consideration public feedback through open forums and written submissions. These public comments provided additional perspectives on the social, ethical, and practical implications of GenAI, ensuring a well-rounded approach to the task force's deliberations.

Definitions

Proper definitions of AI and Generative AI are essential to ensure clarity and consistency in regulation. Illinois enacted legislation that has adopted the following definitions:

"Artificial intelligence" means a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. "Artificial intelligence" includes generative artificial intelligence. (Public Acts 103-0804, 103-0830 and 103-0836)

"Generative artificial intelligence" means an automated computing system that, when prompted with human prompts, descriptions, or queries, can produce outputs that simulate human-produced content, including, but not limited to, the following: (1) textual outputs, such as short answers, essays, poetry, or longer compositions or answers; (2) image outputs, such as fine art, photographs, conceptual art, diagrams, and other images; (3) multimedia outputs, such as audio or video in the form of compositions, songs, or short-form or long-form audio or video; and (4) other content that would be otherwise produced by human means. (Public Acts 103-0804 and 103-0830).

Federal & International Guidance on Artificial Intelligence

This section summarizes key federal and international guidance on AI, drawing from the White House Blueprint for an AI Bill of Rights, Executive Order 14110, “Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence,” the NIST Generative AI Risk Framework, the Department of Homeland Security's (DHS) Roles and Responsibilities Framework, and international frameworks such as the OECD AI Principles and the European Union's AI Act.

U.S. Federal Guidance on Generative AI

The Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, issued in October 2023, establishes a federal framework to govern AI technologies. It prioritizes AI safety, civil rights protections, privacy safeguards, and innovation through public-private collaboration. Federal agencies must address risks in AI systems that impact national security, critical infrastructure, and public well-being, particularly by ensuring that AI systems are transparent, equitable, and privacy-enhanced.

The Blueprint for an AI Bill of Rights, developed by the White House Office of Science and Technology Policy, preceded the Executive Order and outlined five core principles to protect Americans from the harms of AI systems:

1. **Safe and Effective Systems**: AI systems should be tested and monitored to ensure safety, reliability, and effectiveness. Independent evaluations and transparency in safety protocols are essential.
2. **Algorithmic Discrimination Protections**: AI systems should be designed to prevent algorithmic bias and discrimination.
3. **Data Privacy**: Individuals should have agency over their data. AI systems should incorporate safeguards to prevent misuse, including data minimization and consent-based collection practices.
4. **Notice and Explanation**: AI users should be informed about how systems are used and impacted. There should be clear, accessible documentation and explanations of AI decisions.
5. **Human Alternatives, Consideration, and Fallback**: AI systems should allow for human oversight, intervention, and alternative decision-making pathways, ensuring accountability and protection in sensitive contexts.

The National Institute of Standards and Technology (NIST), an agency of the U.S. Department of Commerce, released a Generative AI Risk Management Framework that provides a more technical lens, identifying twelve key risks unique to or exacerbated by generative AI systems. These risks include:

- **CBRN Information or Capabilities**: AI-facilitated access to chemical, biological, radiological, or nuclear weapon designs and information.
- **Confabulation**: The confident generation of false or misleading information.
- **Dangerous or Violent Content**: Content inciting self-harm, threatening, or illegal activity.
- **Data Privacy**: The exposure or misuse of personally identifiable data or other sensitive information.
- **Environmental Impacts**: High energy use associated with training and operating AI systems.
- **Harmful Bias and Homogenization**: Amplification of systemic biases and discrimination.
- **Human-AI Configuration**: Overreliance, emotional entanglement, algorithmic aversion, and deference to AI systems.
- **Information Integrity**: Generation of deepfakes and disinformation that erode public trust.
- **Information Security**: AI-enabled cyberattacks, malware, and adversarial system manipulation.
- **Intellectual Property**: Unauthorized use of copyrighted or proprietary material.
- **Obscene or Abusive Content**: AI-generated harmful content such as non-consensual abusive imagery.
- **Value Chain and Component Integration**: Risks arising from unverified, untraceable third-party components or data sources.

The U.S. Department of Homeland Security released a Roles and Responsibilities Framework focusing on AI deployment in critical infrastructure, emphasizing the shared responsibilities of AI developers, cloud infrastructure providers, critical infrastructure operators, and the public sector. DHS categorizes risks into asset-level, sectoral, systemic & cross-sector, and nationally significant levels, and calls for pre-deployment testing, continuous monitoring, and incident response protocols. The DHS framework highlights AI's dual role in strengthening infrastructure resilience while posing new vulnerabilities to sectors such as healthcare, water systems, transportation, and energy grids.

Additional federal guidance and policies exist, including from the EPA, the Government Accountability Office, and the Office of Management and Budget's (OMB) and other agencies. Together, these documents provide important guidance for governing AI, including Generative AI.

OECD AI Principles

The Organisation for Economic Cooperation and Development (OECD) is an international organization that provides a forum for its 38 member countries to discuss and coordinate

economic and social policies. The United States is a founding member of the OECD, which was established in 1961.

The OECD AI Principles, updated in May 2024, outline key principles including promoting inclusive growth and well-being, respecting human rights and democratic values, ensuring transparency and explainability of AI systems, and maintaining robustness, safety, and accountability throughout the AI lifecycle.

To support these principles, the OECD recommends that policymakers invest in AI research, foster an inclusive AI ecosystem, and create adaptable governance frameworks that promote trustworthy AI. The OECD also recommends that governments take measures to upskill the workforce to prepare for AI-driven labor changes, and encourages international cooperation to address global AI challenges.

European Union AI Act

The EU AI Act introduces a risk-based regulatory approach to AI governance, classifying AI systems into four categories: unacceptable, high, limited, and minimal risk. AI systems with unacceptable risks, such as social scoring or systems undermining fundamental rights, are banned. High-risk AI applications, such as those used in healthcare, law enforcement, and critical infrastructure, are subject to stringent testing, risk assessments, and transparency requirements. Developers must implement bias mitigation strategies, ensure human oversight, and provide clear documentation. Limited-risk systems, such as chatbots, are required to disclose their AI nature, while minimal-risk systems remain largely unregulated to promote innovation.

This overview highlights key federal and international guidance on AI, but the regulatory landscape is rapidly evolving, including with states beginning to develop their own robust AI frameworks and policies.

Labor & Workforce

Artificial Intelligence (AI) is playing an increasingly significant role in the global economy and has the potential to transform workplaces. Generative AI is among the most recent advancements, a subset of AI capable of creating text, images, code, and more. Tools like ChatGPT, DALL-E, and Bard are redefining industries by automating tasks once thought to require uniquely human traits like creativity and critical thinking. For Illinois — a state with a diverse economy spanning manufacturing, transportation, healthcare, finance, and creative industries — the rise of Generative AI presents unique challenges and opportunities for our state's workforce and economy.

This section explores the impact of AI, with a specific focus on Generative AI, on Illinois' workforce, highlights sectors at risk, evaluates existing state initiatives, and provides recommendations for policymakers outlining the need for worker-centric policies to ensure equitable benefits from this powerful technology.

In the Illinois Future of Work Act, signed into law on August 19, 2021, the General Assembly expressed the following position on AI's impact on the workforce: "Rapid advancements in technology, specifically the automation of jobs and expanded artificial intelligence capability, have had and will continue to have a profound impact on the type, quality, and number of jobs available in our 21st century economy. Automation and the rise of artificial intelligence and predictive analytics will have major impacts on industries and their jobs; from the service sector to white collar positions, the impacts will be felt by millions of workers in the United States."

A report[1] by the U.S. Department of Labor captures the trade-offs inherent in the rapid adoption of AI technologies:

> *The precise scope and nature of how AI will change the workplace remains uncertain. AI can positively augment work by replacing and automating repetitive tasks or assisting with routine decisions, which may reduce the burden on workers and allow them to better perform other responsibilities. Consequently, the introduction of AI-augmented work will create demand for workers to gain new skills and training to learn how to use AI in their day-to-day work. AI will also continue creating new jobs, including those focused on the development, deployment, and human oversight of AI. But AI-augmented work also poses risks if workers no longer have autonomy and direction over their work or their job quality declines. The risks of AI for workers are greater if it undermines workers' rights, embeds bias and discrimination in decision-making processes, or makes consequential*

[1] U.S. Department of Labor, ed. 2024. *Artificial Intelligence And Worker Well-being: Principles And Best Practices For Developers And Employers*.

workplace decisions without transparency, human oversight, and review. There are also risks that workers will be displaced entirely from their jobs by AI.

Generative AI tools are now more accessible than ever, providing everyday people with capabilities that were once cost-prohibitive. This accessibility allows small businesses to leverage these tools to drive growth. On the other hand, workers across many industries, particularly in knowledge-based sectors, are exposed to this technology with consequences that are difficult to fully predict.

Key Sectors Facing Disruption from GenAI

According to a March 2023 report[2] by Goldman Sachs, approximately two-thirds of current jobs in the US and Europe are exposed to some degree of AI automation, the equivalent of 300 million jobs worldwide. Administrative and legal professions show the highest exposure to AI (up to 46%), while roles requiring physical labor, such as construction and maintenance, have minimal exposure (6% and 4%, respectively).

A 2022 study[3] by Pew Research similarly found that "19% of American workers were in jobs that are the most exposed to AI, in which the most important activities may be either replaced or assisted by AI."

A shift in the workforce of this magnitude demands the attention of policymakers and regulators, especially since key sectors in Illinois are facing disruption. These include:

Creative Industries

- Marketing and Advertising: Tools like Jasper AI can generate ad copy, social media content, and branding materials, reducing demand for copywriters and graphic designers. Illinois employs[4] over 25,000 professionals in marketing and advertising–the second largest in the country, per capita–many of whom are exposed to this technology.
- Media and Entertainment: Generative AI can produce news articles, scripts, artwork, and video content that challenge traditional creative roles in a sector that contributes significantly to Illinois' economy.

Knowledge Work

- Legal Services: Generative AI like ChatGPT can draft contracts, summarize case law, and conduct legal research, potentially impacting the roles of legal assistants, paralegals,

[2] Briggs, Joseph, and Devesh Kodnani. 2023. "The Potentially Large Effects of Artificial Intelligence on Economic Growth." Goldman Sachs | Economic Research.
[3] Kochhar, Rakesh. 2023. "Which U.S. Workers Are More Exposed to AI on Their Jobs?" Pew Research Institute
[4] Occupational Employment and Wages. May 2023. N.p.: U.S. Bureau of Labor Statistics.

and junior attorneys. Illinois' legal sector employs over 50,000 people, many in roles vulnerable to these advancements.
- Education: AI tools can create lesson plans, grade assignments, and tutor students, impacting teachers' workloads and potentially reducing the need for teacher aides, tutors, and other school support staff. This technology could affect the state's educators and paraprofessionals.

Technical and Professional Services

- Software Development: Generative AI like GitHub Copilot assists in writing and debugging code, reducing the time and need for junior developers in Illinois' burgeoning tech industry.
- Healthcare Administration: Generative AI automates administrative tasks like patient record summaries and billing queries, affecting ancillary roles in Illinois' healthcare workforce.

Illinois administrative, creative, and knowledge-based workers could become increasingly vulnerable to displacement, especially those without advanced technical skills. The rapid evolution of Generative AI risks rendering some skills obsolete and exacerbating existing inequalities. Where AI literacy may be lacking, workers should be empowered and gain skills through retooling programs that ultimately close an ever-widening digital divide so that the workforce retains a competitive edge.

In addition, Generative AI's ability to produce creative work threatens professionals' intellectual property rights and raises ethical concerns about originality and authenticity. This is particularly relevant in Illinois' arts, design, and entertainment industries, which rely on human creativity. Performing artists risk having their own faces, voices, and bodies exploited through non-consensual digital harvesting and manipulation.

Addressing AI's Impact on the Workforce

Illinois has taken critical steps to address AI's impact on the workforce, including:

1. Artificial Intelligence Video Interview Act (AIVIA): Aimed at ensuring transparency, AIVIA requires employers to disclose and obtain consent for AI use in video interviews, protecting job applicants from algorithmic biases.

2. Illinois Human Rights Act Amendments (Public Act 103-0804): Legislation signed into law in August 2024 prohibits discriminatory use of AI in employment decisions, reinforcing Illinois' commitment to fair labor practices.

3. Right of Publicity & Digital Likeness: Illinois has enacted laws addressing the unauthorized use of individuals' digital likenesses in response to advancements in AI and generative technologies. House Bill 4875 amends the Illinois Right of Publicity Act to prohibit the creation and distribution of "digital replicas"— AI-generated representations of a person's voice, image, or likeness that could mislead others into believing they are authentic — without the individual's consent. House Bill 4762 invalidates contractual provisions that allow the creation and use of digital replicas without proper consent, particularly when agreements lack clear descriptions of intended uses and were negotiated without legal or union representation. These laws protect individuals, particularly those in the creative industries, from exploitation.

4. Illinois' Workers Rights Amendment: In 2022, Illinois voters approved a constitutional amendment that enshrined the fundamental right to organize and bargain collectively for wages, hours, working conditions, and safety protections into the Illinois Constitution. This amendment guarantees that all workers have the right to unionize.

Recommendations

To address additional challenges posed by Generative AI, policymakers should consider measures that protect workers from displacement while preparing the workforce for AI innovation. The state should invest in training programs to help workers transition to new roles created by AI, focusing on digital skills and collaboration with AI tools. Partnerships with unions, industry leaders, and academic institutions can ensure workers have a voice in shaping policies that address these challenges.

The U.S. Department of Labor has outlined a set of principles, reproduced below, for deployers of AI to ensure worker well-being:

- [North Star] Centering Worker Empowerment: Workers and their representatives, especially those from underserved communities, should be informed of and have genuine input in the design, development, testing, training, use, and oversight of AI systems for use in the workplace.
- Ethically Developing AI: AI systems should be designed, developed, and trained in a way that protects workers.
- Establishing AI Governance and Human Oversight: Organizations should have clear governance systems, procedures, human oversight, and evaluation processes for AI systems in the workplace.
- Ensuring Transparency in AI Use: Employers should be transparent with workers and job seekers about the AI systems used in the workplace.

- Protecting Labor and Employment Rights: AI systems should not violate or undermine workers' rights to organize, health and safety rights, wage and hour rights, and anti-discrimination and anti-retaliation protections.
- Using AI to Enable Workers: AI systems should assist, complement, enable workers, and improve job quality.
- Supporting Workers Impacted by AI: Employers should support or upskill workers during AI-related job transitions.
- Ensuring Responsible Use of Worker Data: Workers' data collected, used, or created by AI systems should be limited in scope and location, used only to support legitimate business aims, and protected and handled responsibly.

These policies should be the basis for worker-centered AI policy in Illinois. In addition, policymakers should:

- Ensure proper enforcement of recently enacted legislation designed to protect workers from risks posed by the proliferation of AI tools
- Continue to study the risk to Illinois' workforce from the rapid adoption of AI technologies.
- Outlaw workplace surveillance for monitoring worker organizing or using AI to make behavioral predictions
- Require employers who surveil employees to disclose their use of data collection so workers can be aware of how their data are being collected and used
- Regulate employer use of automated decision-making systems to prevent dangerous risks to the safety, security, or health of workers, clients, or the public that may result from automated decisions related to staffing
- Prevent public service agencies from relying exclusively on automated decision-making systems in making decisions regarding benefits and services or enforcement of laws, ordinances, and rules
- Work with the Illinois Department of Commerce and Economic Opportunity and other workforce agencies to incorporate AI training into workforce programs.
- Work with higher education agencies and institutions to produce certificate programs related to AI skills for employees.
- Explore providing computing power to researchers and businesses

Civil Rights and Civil Liberties

Generative artificial intelligence (GenAI) is a powerful tool for creating convincing misinformation. A.I. tools make it easy to fabricate fraudulent high quality images, videos, and audio in a very short period of time for little to no cost. This new ability for anyone with access to the internet to generate convincing misinformation poses a number of serious threats.

Notably, those threats include the ability to generate non-consensual deepfakes using GenAI, the algorithmic bias found in the way AI is deployed by corporations, and the possibility that bad actors will use AI to interfere in our elections.

Deepfakes and Elections

One particularly concerning threat posed by this new technology is the potential use of GenAI generated misinformation to undermine our elections. In particular, deepfakes, or GenAI generated content that depicts a person doing or saying something that they never actually did in real life, are already being used by some in attempts to influence the outcome of elections.

There was a particularly alarming example of this earlier this year, in Slovakia, where just two days before a major election, a fraudulent audio deepfake of one of the two-party leaders was disseminated relatively broadly on social media. This deepfake audio made it sound like the party leader was discussing how they could rig the election. The depicted candidate went on to lose the election by a small margin[5].

There were many[6] deepfakes circulated in the run up to the November 2024 elections in the United States. One case that gained a great deal of attention was an audio deepfake of President[7] Biden that was circulated via robocall to voters in New Hampshire during the primary. The deepfake made it sound like President Biden was telling voters not to vote. There were many other concerning examples that got much less attention. For example, in North Carolina's sixth congressional district, a PAC supporting one of the candidates in their congressional primary circulated a deepfake of their candidate's opponent saying that he was not fit for office and predicting that his opponent would win the election.[8]

---

[5] CNN. (2024, February 1). *A fake recording of a candidate saying he'd rigged the election went viral. Experts say it's only the beginning.*

[6] CASMI. (2024, January 26). *Tracking political deepfakes: New database aims to inform, inspire policy solutions.*

[7] NPR. (2024, May 23). *A political consultant faces charges and fines for Biden deepfake robocalls.*

[8] News & Observer. (2024). *'Deepfake' videos target Mark Walker in NC congressional campaign.*

Deepfake technology poses a significant threat to our democracy and our elections. It is not hard to envision a nightmare scenario where a well-timed fraudulent deepfake swings the outcome of an election.

New legislation is needed to regulate the use of deepfakes in election communications. It should include the following:

Disclosure Requirements: The proposed legislation should require that any person knowingly circulating a deepfake in an election communication to clearly and conspicuously disclose that the content is a deepfake. This ensures transparency for voters and mitigates the risk of misinformation.

Timing and First Amendment Considerations: To balance the regulation of deepfakes with First Amendment protections, this legislation should only take effect within a defined period leading up to election day, such as 90 days. Implementing this time frame helps to focus the legislation on the critical period when misinformation can have the most significant impact, while also reducing potential conflicts with free speech rights. It is important to recognize that while lying in political speech is constitutionally protected, there is a critical distinction between a lie and a deepfake. A lie can be countered through speech or factual rebuttals; however, deepfakes involve the manipulation of a person's likeness to create fraudulent audio, image, or video content—forms of media that society traditionally relies upon as evidence. Such content portrays individuals as saying or doing things they never actually said or did, making it far more difficult to refute.

Scope and Applicability: The legislation should apply to all individuals who might circulate a deepfake with the intent to deceive voters or undermine the reputation of a candidate, not just candidates and Political Action Committees (PACs). One of the most dangerous scenarios is when a social media influencer with millions of followers uses their platform to distribute a deepfake to influence an election. Therefore, this law must have a broad scope to include anyone attempting to mislead the electorate.

Defining Deepfakes: A clear and consistent standard for what constitutes a deepfake is essential. The legislation should define a deepfake as content that depicts a person doing or saying something they did not actually do or say and that appears real to a reasonable person. This definition should exclude minor cosmetic alterations, such as blemish removal, which do not fundamentally alter the perception of the content. A precise definition will help enforce the law effectively and avoid ambiguity.

Injunctive Relief and Enforcement: The proposed legislation must establish the right for affected parties to seek injunctive relief. This is particularly important when a deepfake is circulated close to an election, as rapid action may be needed to remove misleading content and

dispel misinformation effectively. Enabling timely removal of harmful content is critical to protect the integrity of the electoral process.

Exceptions for Satire and Parody: Finally, it is important to include exceptions for satire and parody as a precaution for First Amendment protections. These forms of expression are protected speech and play an important role in political discourse. Ensuring that these exceptions are clearly defined will help preserve free expression while still addressing the serious risks posed by deceptive deepfakes.

Legislation to regulate the use of deepfakes in election communications has been enacted in 20 states thus far.

In the 103rd General Assembly, three bills (SB 1742, HB 4933, HB 4644) were introduced in Illinois to address this issue, but none have been enacted to date. Passing legislation to regulate deepfakes in election communications remains an urgent priority.

Intimate Deepfakes

Another pernicious use of GenAI that is already affecting many people is the utilization of non-consensual intimate deepfakes to harass, humiliate, threaten or otherwise harm people. An intimate deepfakes is content that has been fabricated using GenAI technology that depicts a person nude or engaging in a sexual act. There has been an exponential rise in the circulation of this type of content. A 2023 study[9] found that 98 percent of online deepfake videos were pornographic, and many of these are generated without the consent of the person being depicted. The vast majority of the victims of non-consensual intimate deepfakes are women and children[10].

This issue is much more widespread than many people realize. Thirteen percent of teens[11] say they have some sort of experience with nude deepfakes. On Telegram alone, there are at least 50 bots that claim to create explicit photos or videos of people with only a couple of clicks — these bots have over 4 million monthly users[12].
Intimate deepfakes cause serious harm to innocent people[13]. Victims report experiencing significant emotional consequences[14] and trauma, as well as damage to their reputation and career.

[9] SecurityHero. (2023). *State of deepfakes: Appendix.*
[10] Glamour. (2024). *It's Not Just Taylor Swift—All Women Are at Risk From the Rise of Deepfakes.*
[11] Internet Matters. (2024). *The new face of digital abuse: Children's experiences with nude deepfakes.*
[12] Wired. (2024). *Millions of People Are Using Abusive AI 'Nudify' Bots on Telegram.*
[13] National Sexual Violence Resource Center (NSVRC). (2024). Taylor Swift and the dangers of deepfake pornography.
[14] Urban Survival. (2024). *The psychological effects of AI clones and deepfakes.*

Illinois has taken significant steps to address the issue of deepfakes through the passage of three laws: HB 2123 (Public 103-0294), SB 382 (Public Act 103-0571), and HB 4623 (Public Act 103-0825). These laws provide strong protections against the malicious distribution of intimate deepfakes. The Illinois State Board of Education, the Board of Higher Education, and other agencies should work with high schools, community colleges, and universities to ensure young people, who are at higher risk of exposure to this technology, are aware of these laws. Robust enforcement will also be important.

Algorithmic Bias

Artificial Intelligence (AI) algorithms are increasingly being employed in decision-making processes across sectors. These systems are used to rank, classify, and make determinations about individuals in ways that have significant and far-reaching effects on their lives, particularly in critical areas such as healthcare, housing, employment, education, and financial services.

The widespread use of Generative AI models raises concerns due to the potential for biased and discriminatory outcomes. Bias is inherent in GenAI systems for two primary reasons: they are trained on data sets that often reflect historical and societal biases, and the humans responsible for training and designing these systems carry their own implicit biases.

These systems are now being used in many high-stakes decision-making areas, such as hiring processes, loan pricing, and mortgage approvals—decisions that fundamentally impact individuals' opportunities and quality of life. By automating these processes, GenAI systems risk perpetuating or exacerbating existing biases and discrimination, embedding systemic inequalities more deeply into decision-making frameworks.

A significant challenge in addressing this issue lies in the lack of transparency surrounding GenAI systems. There is often little insight into how these models are trained, how they function, and the factors they consider when making decisions. This opacity makes it difficult to identify, challenge, or correct biases embedded in AI-driven outcomes.

As the use of GenAI in critical decision-making roles continues to expand, these biases could become further entrenched unless meaningful guardrails and regulations are enacted. To address these challenges, additional legal protections are needed to promote transparency, accountability, and fairness.

To effectively address algorithmic bias, the Task Force recommends the following measures aimed at promoting transparency, accountability, and fairness in AI systems.

Extension of Civil Rights Laws: Existing civil rights laws must be explicitly extended to address harmful impacts resulting from AI-driven decisions. This is a critical step in ensuring that individuals are protected from discriminatory outcomes produced by automated systems.

Transparency in AI Use and Decision-Making: Laws should mandate transparency regarding the deployment of AI systems, particularly in areas that have a significant impact on people's lives. This includes requiring clear notice of how decisions are made, with specific details on how inputs are weighted and contribute to the final outcome. Additionally, the data sets used to train AI models must be disclosed to allow for scrutiny and to identify potential biases.

Appropriate Definitions: It is essential to develop clear, precise definitions of GenAI and algorithmic systems. These definitions must thoughtfully encompass the full scope of technologies being used in high-impact areas, ensuring legal frameworks remain relevant and effective.

Mandatory Assessments and Audits: Developers and deployers of AI systems that affect people's lives must be required to implement comprehensive assessment protocols. These include mandatory pre- and post-deployment audits to evaluate system bias, fairness, and effectiveness. To promote transparency, these audits should be published and made available to the public. Importantly, the audits must be conducted by independent auditors to ensure objectivity and integrity throughout the process.

Human Oversight: Human oversight is crucial in GenAI decision-making. There should be a human decision-maker in the loop with the authority to challenge, review, or overturn the outcomes of GenAI systems. This oversight helps mitigate potential harm and ensures accountability in automated decision-making processes.

Individual Rights and Accountability: Individuals must have the right to challenge GenAI-driven decisions, particularly those with significant impacts on their lives. To further strengthen accountability, a private right of action should be established, allowing individuals to seek legal recourse when harmed by the decisions or outcomes of GenAI systems.

Consumer Protection

Data Privacy

Generative Artificial Intelligence (GenAI), while offering unprecedented capabilities to create, analyze, and synthesize content, raises significant concerns for consumer privacy. These concerns stem from the collection, processing, and dissemination of vast quantities of personal data, often without sufficient oversight or consumer consent. As GenAI systems become increasingly integrated into consumer-facing technologies, the risks to personal privacy grow, necessitating regulatory attention and policy intervention.

Illinois has been at the forefront of protecting biometric information through its Biometric Information Privacy Act (BIPA), which requires companies to obtain explicit consent before collecting biometric data and imposes penalties for misuse. This model provides a strong foundation for broader privacy protections, particularly as generative AI systems increasingly process biometric data such as facial recognition and voice patterns.

GenAI systems, such as large language models and image generators, are trained on massive datasets, which often include sensitive personal information sourced from online platforms, databases, and public spaces. The White House's AI Bill of Rights emphasizes the importance of data privacy, stating that individuals have the right to protect their personal data and control how it is used. However, generative AI's reliance on vast and often unstructured datasets poses a threat to this goal. Personal data can inadvertently become part of training datasets without consumer knowledge or explicit consent, leading to privacy breaches.

A 2024 Deloitte's survey on consumer privacy and security found that "Nine in 10 people surveyed think they should be able to view and delete the data companies collect on them. 90% say technology companies should do more to protect their data, and 84% say the government should do more to regulate the way companies collect and use consumer data, as well."

GenAI tools are increasingly capable of capturing and analyzing data from public and semi-public spaces. Technologies such as AI-powered surveillance systems and voice recognition tools can gather personal data, often without individuals realizing they are being monitored. This capability undermines the assumption of privacy in shared spaces, contributing to a broader erosion of personal privacy rights.

Consumer Fraud

GenAI also poses significant risks of fraud and deception. Tools capable of creating highly realistic text, images, and audio have been increasingly used to commit financial fraud, identity

theft, and other deceptive activities. For instance, GenAI-generated voice clones have enabled scammers to impersonate trusted individuals, such as family members or business leaders, to manipulate victims into transferring money or disclosing sensitive information. Similarly, deepfake images or videos can be used to falsify identification documents or carry out social engineering attacks. Collaborative efforts between regulatory bodies, AI developers, and financial institutions are essential to create effective safeguards against GenAI-driven fraud.

Chat Bots

GenAI chatbot technology has advanced rapidly, reaching a point where it can engage in conversations that are strikingly human-like. These chatbots are capable of carrying on discussions in ways that can easily lead users to believe they are speaking with a real person. Programmed to exhibit human qualities, chatbots can provoke emotional responses and create the illusion of empathy, further blurring the line between artificial and human interaction.

In addition to their conversational abilities, chatbots can be fine-tuned for persuasion and manipulation. Many are designed to use data they collect from users to learn how to influence them more effectively. This data-driven approach allows chatbots to subtly guide user behavior, whether it's encouraging continued engagement, promoting product purchases, or serving other goals set by their developers and deployers.

Currently, there are no widespread requirements for consumers to be informed when they are interacting with a chatbot, leading to significant ethical concerns. For instance, a user may believe they are speaking with a licensed professional, such as a medical expert, financial advisor, or therapist, when, in fact, they are communicating with an AI-driven system. This lack of transparency raises critical issues around trust, consent, and the potential for exploitation in sensitive areas of personal interaction.

Recommendations

To address the privacy challenges posed by GenAI, policymakers should implement the following recommendations:

- **Data Privacy Rights:** Policymakers should take measures to give consumers control over their personal data, including protecting consumers from the sale or sharing of their data without clear and informed consent. Companies deploying GenAI tools should be required to provide robust privacy guarantees, ensuring that sensitive personal information is neither shared with third parties nor sold for profit. Developers should provide clear disclosures about how personal data is collected, used, and stored. Adopting the principles outlined in the AI Bill of Rights, consumers should have the right to access,

delete, or opt out of GenAI systems processing their data. User-friendly tools that empower individuals to exercise these rights should be widely accessible.

- **Strengthen Data Anonymization Requirements** To prevent the inadvertent exposure of personal information, companies should adopt stronger data anonymization standards. Policies should ensure that data used for training GenAI models undergo rigorous anonymization to ensure no identifiable personal information remains. Regular audits and third-party oversight can help ensure compliance.

- **Transparency**: Consumers should have a right to be informed when they are interacting with a chatbot or other human-seeming technology. Legislation should be enacted to make it an unfair or deceptive trade practice for a consumer to interact with human seeming technology or chatbot that a reasonable person would believe is an actual human without being notified.

- **Implement Restrictions on AI Use in Public Spaces:** Policymakers should implement regulations to restrict the use of GenAI for data collection in public and semi-public spaces. Surveillance technologies powered by GenAI must be subjected to strict oversight to prevent privacy invasions and ensure compliance with ethical standards.

Environment & Sustainability

Generative AI (GenAI) has revolutionized industries, but its continued development comes with environmental challenges. By one estimate, the amount of computational power required to sustain GenAI is doubling roughly every 100 days.[15] This section outlines the environmental impacts associated with GenAI, notably energy consumption, carbon emissions, water usage, and e-waste generation. It also provides policy recommendations for lawmakers with the goal of reducing the environmental impact of GenAI, while balancing its continued importance in the state's economy.

The energy demands of training and deploying large AI models are a growing environmental concern. Training advanced models like GPT-4 or DALL·E involves processing extensive datasets across thousands of servers for weeks or months. These training processes consume enormous amounts of electricity, often sourced from fossil fuels, leading to substantial carbon emissions.[16]

Once deployed, these models require continuous computational power for inference, where they generate outputs in real-time for millions of users. This persistent demand for resources intensifies the environmental footprint of GenAI applications. The International Energy Agency estimates that the AI-related electricity demand will increase at least tenfold by 2026[17].

The Negative Environmental Impact of GenAI

GenAI systems rely on data centers to perform computations and store information. These centers consume massive amounts of energy to power servers and maintain optimal operating temperatures. Cooling mechanisms, essential for preventing data centers from overheating, require substantial water usage. According to research from the University of California, a single AI prompt can consume as much cooling water as a 16.9 oz bottle of water.[18]

GenAI is exacerbating local resource scarcity. In water-stressed regions, the need to cool data centers places a heavy strain on communities and ecosystems.[19]

The hardware requirements of GenAI contribute to increasing levels of electronic waste. High-performance components such as GPUs and TPUs are critical for AI operations but have limited

[15] Intelligent Computing. (2023). *Intelligent Computing: The Latest Advances, Challenges, and Future.*
[16] Stanford Institute for Human-Centered Artificial Intelligence. (2023). *Artificial Intelligence Index Report 2023.*
[17] International Energy Agency. (2024). *Electricity 2024: Analysis and Forecast to 2026.*
[18] OECD Artificial Intelligence Policy Observatory. (2023). *How much water does AI consume? The public deserves to know.*
[19] Forbes. *AI Is Accelerating the Loss of Our Scarcest Natural Resource: Water.*

lifespans due to rapid technological advancements. Frequent hardware upgrades lead to significant e-waste generation, with much of it being non-recyclable or containing hazardous materials. Without adequate recycling initiatives, this waste accumulates in landfills, posing long-term environmental risks.[20]

Recommendations

To address these environmental challenges presented by GenAI, stakeholders should consider the following actions:

Evaluate Incentives for Sustainable Data Centers: At the state level, Illinois should explore policies that incentivize environmentally sustainable data centers through renewable energy adoption, improved energy and water efficiency, responsible site selection, and transparent environmental reporting. By evaluating and refining existing tax credits, grants, or subsidies for data centers, the state can reduce emissions and promote sustainable growth in the digital economy.[21]

Strengthen Transparency and Accountability: To enhance the environmental transparency of data centers in Illinois, the state should assess current reporting practices and engage with industry stakeholders to develop standardized metrics for energy consumption, water usage, and waste management. Establishing reporting guidelines for data centers will encourage accountability and sustainability. By creating clear frameworks for transparent reporting, the state can ensure that data centers contribute to Illinois' broader climate objectives while driving responsible business practices.

Encourage Hardware Recycling and Circular Economy Practices: Illinois should implement policies that promote hardware recycling and circular economy practices within the AI and tech industries. This includes mandating the recycling of obsolete hardware, incentivizing the reuse of components, and expanding e-waste recycling infrastructure.[22] By fostering a sustainable hardware lifecycle, Illinois can help mitigate the environmental impact of GenAI and encourage more sustainable tech development.

Establish Monitoring and Promote Innovation: Illinois should establish a state-level commission to monitor GenAI's environmental impact and propose regulations and initiatives to help reduce GenAI's carbon footprint while growing the state's tech economy. Additionally, the

[20] MIT Technology Review. (2024). *AI will add to the e-waste problem. Here's what we can do about it.*
[21] HWG LLP. (2024). *How Global Data Center Regs May Influence U.S. Policies.*
[22] The Baker Institute for Public Policy: Center for Energy Studies. (2023). *Closing the Loop on the World's Fastest-growing Waste Stream: Electronics.*

state should adopt best practices from both domestic and international models to ensure Illinois data centers align with state and national climate goals.

Expand Renewable Energy Production: Illinois should continue to invest in building new sources of renewable energy to meet its goal of transitioning to an equitable, reliable, and cost-effective clean electricity system. The size of the GenAI's carbon footprint is highly dependent on regional access to renewable energy sources like wind and solar.[23] In order to reduce the environmental impact of GenAI in Illinois, policymakers need to prioritize green investment and aggressively expand clean energy production in the state. Additionally, Illinois should ensure that the energy needs of GenAI are factored into its Renewable Energy Access Plan (REAP).

Promote Research Into Possible Environmental Benefits of AI: While this section focused on the environmental toll of GenAI, GenAI may be a useful tool to help mitigate the impacts of climate change by improving weather forecasting, helping to predict climate disasters, and even making waste management more efficient.[24] Illinois could provide grants to universities, think tanks, and other institutions that are researching ways in which AI could assist in environmental monitoring and management.

[23] Harvard Business Review. (2024). *The Uneven Distribution of AI's Environmental Impacts.*
[24] World Economic Forum. (2024). *9 ways AI is helping tackle climate change.*

Higher Education

Illinois is home to a diverse array of higher education institutions that share a common mission: providing students with opportunities to advance their knowledge and grow as individuals.

This section contains proposals for clear, well-developed guidelines around the use of Generative AI for faculty, staff, and students. These recommendations incorporate information from presentations to the task force, feedback from the higher education community, research by task force members, and direction from the Illinois Board of Higher Education's strategic plan, *A Thriving Illinois – Higher Education Paths to Equity, Sustainability, and Growth.*

Ethical Use

The rise of Generative AI (GenAI) presents significant ethical challenges for institutions of higher education. Without clear and consistent policies, campuses may face a range of issues, including:

- **Harmful Content Creation:** The potential misuse of GenAI to produce discriminatory, deceptive, or otherwise harmful content could negatively impact individuals and the broader campus environment.
- **Lack of Reporting Mechanisms:** Inadequate channels for reporting unethical use of GenAI, both within and outside the classroom, can leave harmful behaviors unaddressed and diminish trust in the campus community.
- **Inadequate Resolution Processes:** The absence of formalized complaint and appeal processes leaves those affected by GenAI decisions without proper recourse or resolution.
- **Privacy Risks:** Sharing personally identifiable information (PII) on publicly accessible GenAI systems exposes institutions to serious privacy concerns and potential legal liabilities.
- **Disjointed Technology Adoption:** A lack of centralized oversight for approved GenAI services across campus can result in inconsistent implementation and potential security vulnerabilities.
- **Ambiguity in Classroom Use:** The absence of clear institutional policies on how faculty may use GenAI in the classroom creates confusion and inconsistency in student expectations.
- **Unclear Research Guidelines:** Researchers and scholars may inadvertently misuse GenAI tools without standardized guidance on ethical and transparent usage.

Without a coordinated effort to address these concerns, institutions risk fostering environments where misuse of GenAI could proliferate, and accountability remains unclear. Furthermore, the absence of diverse stakeholder input in policy creation could lead to policies that fail to represent the needs of the entire campus community.

Equitable Access & AI Literacy

Access to Generative AI technology is essential for preparing students for the demands of an evolving workforce. However, significant barriers exist, particularly for low-income students, such as:

- **Barriers to Access:** The lack of institutional access to large language model GenAI services may disadvantage students from underprivileged backgrounds, widening the equity gap.
- **Lack of Baseline AI Literacy:** Without training opportunities, students may struggle to develop basic AI literacy, leaving them unprepared for the integration of these technologies in both academic and professional settings.
- **Faculty and Staff Knowledge Gaps:** Faculty and staff often lack the training and professional development necessary to incorporate AI tools effectively and ethically into their work, reducing the quality of education and administrative practices.

Failure to address these inequities risks exacerbating existing disparities and leaving students underprepared for future opportunities.

Recommendations

We recommend that the Illinois Board of Higher Education and the Illinois Community College Board collaborate with institutions of higher learning on the following:

Establish Clear Policy Frameworks and Guidelines: Develop and promote model policies to guide institutions in the ethical, responsible, and transparent use of Generative AI (GenAI). These frameworks should address key issues, including data privacy, intellectual property, academic integrity, and compliance with existing laws, such as FERPA and copyright regulations.

Provide Guidance for AI Integration in the Classroom: Create resources to support faculty in incorporating GenAI tools into their teaching practices, as well as clear guidelines for students on the acceptable use of AI in assignments and collaboration. Additionally, offer strategies to uphold academic integrity, such as leveraging AI detection tools and fostering discussions about the ethical implications of GenAI in education.

Facilitate Training and Resource Access: Organize professional development workshops to train educators and administrators on effectively using GenAI tools. Ensure institutions have access to vetted AI platforms that adhere to educational and ethical standards, enabling safe and impactful adoption of these technologies.

Encourage Research and Innovation: Allocate funding and grants to research the impact of GenAI on education and its potential to enhance learning outcomes.

P-12 Education

The use of AI in P-12 schooling is both nascent and emergent due to the changing landscape of the technology and the 'time-lag' in importing new possibilities into the P-12 system. States[25] and other organizations have been carefully tracking the current research in AI in schooling, including the necessary support schools require for the equitable and responsible student and educator use of AI technology.[26]

To support Illinois districts in the responsible use of AI as well as meeting specific aspects of the Generative AI and Natural Language Processing Task Force charge,[27] working group members identified the following problem statement:

Illinois school districts face the complex challenge of leveraging the potential benefits of generative artificial intelligence (AI) for purposes of teaching and learning and district and school operations while mitigating its risks. These challenges necessitate a comprehensive approach that balances innovation with responsible implementation.

The problem statement captures the need for guidance, materials, and resources to Illinois public school educators, students and other stakeholders on navigating the use of AI.

Surveying Educators

National[28] and international[29] surveys of those who work in the P-12 system reinforce the need for state-level guidance, materials, and training. The themes identified in the surveys were supported through data collection on GenAI with members of the Illinois Association of School Administrators (IASA) and Illinois Principal Association (IPA)[30] in August 2024.[31]

Respondents were surveyed on GenAI awareness, use, policy and leadership, safety, and ethics. A summary of findings can be found in Appendix B and can be considered when developing model policies, resources and related materials for specific audiences (e.g., district and school leaders, classroom teachers, parents and caregivers, students).

[25] Appendix A.1
[26] Appendix A.2
[27] Appendix A.3
[28] Appendix A.4
[29] Appendix A.5
[30] Appendix A.6
[31] Appendix A.7

A November 2024 "Rules and Tools for AI-Powered Learning" report by Teach Plus and the Illinois Digital Educators Alliance emphasizes the need for regulations that balance flexibility for exploration with protections for students, ensuring their learning experiences and safety remain a top priority. Educators also express a strong desire for professional development to effectively use AI tools and teach students about responsible usage while addressing equity concerns to ensure all students have access to these technologies.[32]

School District Policies

Some school districts have taken proactive steps to develop their own policies for the ethical and effective use of generative AI. These include Chicago Public Schools, Township High School District 211, and Indian Prairie School District 204.[33] [34] [35] School districts that are in the process of developing their own guidelines can gain valuable insights by studying their peers' policies and adapting them to their own context.

The generative AI policies from various school districts share several key themes:

1. **Ethical and Responsible Use**: The importance of using AI tools ethically, responsibly, and in alignment with academic integrity is highlighted. This includes citing AI-generated content appropriately when used in educational work.
2. **Privacy and Security**: Safeguarding personal and sensitive information is a central concern, with explicit guidelines to avoid sharing personally identifiable data while using AI tools.
3. **Educational Enhancement**: The potential of AI to enrich learning experiences is acknowledged, encouraging its use for personalized learning, creative problem-solving, and support in research or content generation.
4. **Critical Evaluation and Information Literacy**: Emphasis is placed on fostering critical thinking skills to evaluate AI-generated content and ensuring students can assess the credibility and reliability of such information.
5. **Professional Development and Capacity Building**: Resources and training for educators are prioritized to help integrate AI tools effectively into teaching practices while building readiness and expertise.
6. **Policy Evolution and Continuous Improvement**: Regular reviews and updates are planned to keep the policies relevant, reflecting new insights, stakeholder feedback, and technological advancements.

[32] Appendix A.10
[33] Chicago Public Schools. *AI Guidebook*
[34] Township High School District 211. *Artificial Intelligence Guidelines*
[35] Indian Prairie School District 204. *Generative AI Guidelines*.

These policies aim to responsibly integrate AI in education while balancing innovation with ethical considerations and safeguarding privacy.

Recommendations

The Illinois State Board of Education should issue comprehensive guidance to school districts, incorporating the following themes and principles:

- **AI Use and Integration**: ISBE should provide guidance on the use of AI tools to support educational objectives. This should include recommendations for navigating AI tools that offer personalized learning experiences. Additionally, ISBE should outline best practices for incorporating AI into administrative tasks, such as lesson planning or grading, to allow educators to focus more on student engagement. Resources should be made available to help districts evaluate AI tools for their effectiveness and alignment with state standards.

- **AI Literacy:** To prepare students for a world increasingly influenced by AI, ISBE should provide curricular frameworks for teaching AI literacy. This includes ensuring students understand the basics of AI, its applications, and its broader social implications. Encouraging critical thinking about the implications of AI on privacy, employment, and decision-making is an essential part of fostering informed and responsible future citizens.

- **Ethical and Equitable AI Implementation:** ISBE should outline strategies for implementing AI tools ethically and equitably in schools. Clear standards for transparency should be established so that educators, students, and parents understand how AI systems operate. Additionally, districts should be encouraged to ensure that AI tools are accessible to all students, including those from underserved communities and those with disabilities.

- **Data Privacy and Security:** Given the sensitive nature of student data, ISBE should develop protocols for safeguarding privacy in AI systems. Guidance should include best practices for data collection, storage, and sharing, ensuring compliance with state and federal privacy laws. ISBE could also provide resources to districts to help them educate stakeholders—educators, parents, and students—about the implications of using AI technologies that rely on large amounts of data.

- **Professional Development for Educators:** ISBE should consider offering training programs and professional development opportunities for educators. These initiatives could help teachers understand how to use AI tools responsibly and effectively in their

classrooms and for administrative tasks. Ongoing support and the establishment of a statewide professional learning network could also help educators share best practices and address challenges associated with AI.

- **Monitoring and Accountability:** ISBE should recommend strategies for districts to evaluate the impact and effectiveness of AI tools, including metrics for assessing academic outcomes, student engagement, and equitable access. Periodic reviews of AI policies at the state level would ensure they remain relevant in light of technological advancements.

In addition, we recommend that ISBE conduct regular surveys to gather feedback and insights to refine its guidance, use extant systems (e.g., Regional Offices of Education and Intermediate Service Centers, Learning Technology Centers) to deliver training through a variety of modes (e.g., train the trainer models, synchronous training, asynchronous trainings, microcredentials affixed to a Professional Educator License), and curate a website on which state-developed and national resources are available to school districts. Finally, we recommend ISBE revise or create new Illinois Professional Educator Standards to ensure that higher education programs that prepare teachers and teacher candidates are trained to navigate the complexities of AI in instructional settings.

Cybersecurity

Artificial Intelligence (AI) and Natural Language Processing (NLP) present unique cybersecurity risks to Illinois institutions and users. This section covers risk management at three different levels of analysis: the system/software level, user/organization level, and societal level.

System Level: At this level, most security concerns are related to the security of the GenAI systems and their underlying data and algorithms. Examples of potential security risks include (but are not limited to) the following:

- **Violations of model integrity:** In these situations, the underlying models can be tricked to provide unauthorized outputs (prompt injection, jailbreaking) or the model behavior can be altered (training data poisoning, repurposing of a pre-trained model).
- **Violations of data integrity:** In these situations, either the underlying training data used to tune the models is exposed (data exfiltration) or the additional organization-specific data used to fine-tune the models is exposed (privacy compromise).

User/Organization Level: Legitimate GenAI tools have the potential to be used in unintended and malicious ways, including (but not limited to) the following:

- **Realistic depictions of humans:** Deepfakes, appropriated likeness, synthetic online personas (e.g., "troll farms") and the creation of sexually explicit content.
- **Falsification of non-human entities:** the creation of misinformation, falsified evidence or counterfeit materials
- **Increased cybercrime**: the use of GenAI for scaling and improvement of certain cyberattacks, such as spam and phishing emails.

Societal Level: The best GenAI models require vast amounts of data and computing resources to train and run. This potentially opens up a broader discussion about whether major GenAI providers should be treated as public utilities to ensure fair access for everyone. From the cybersecurity standpoint, this can lead to a rise in supply chain attacks:

- Supply chain attacks take advantage of a broader platform serving multiple clients. By targeting the platform provider, an attacker can cause damages to multiple clients simultaneously – ranging from a denial-of-service attack to model poisoning.

Risk Management Frameworks and Standards

The NIST AI Risk Management framework is particularly well-suited to addressing AI and NLP risks, offering specific guidance for identifying, mitigating, and monitoring risks throughout the AI lifecycle. This standard offers a flexible, risk-based approach tailored to AI systems, emphasizing accountability, fairness, and transparency. It is organized into four functions:

- **Map:** Identifying AI-specific risks, including biases in NLP datasets or malicious data inputs
- **Measure:** Developing metrics for system performance and potential vulnerabilities in NLP models

- **Manage:** Implementing risk mitigation strategies to address identified threats
- **Govern:** Overseeing processes for continuous evaluation and improvement

In addition, there are several individual controls and frameworks available that should be considered when developing an AI and NLP risk management program / assessment:

- **Data Security and Privacy (ISO/IEC 27001 Annex A.8):** Validating that the integrity and confidentiality of NLP training data manages risks of poisoning or privacy violations. Controls, including differential privacy and data anonymization, should be considered.
- **Access Control and Monitoring (ISO/IEC 27001 Annex A.9):** Restricting access to NLP models / training data and monitoring usage of models prevents unauthorized exploitation and tampering.
- **Model Robustness Testing (NIST AI RMF):** Periodically testing NLP models for robustness against adversarial inputs exposes risks in AI and NLP enabled systems, allowing engineers to protect exploitation. Fuzz testing can reveal vulnerabilities in chatbot or voice recognition systems.
- **MITRE ATLAS Matrix:** Similar to the MITRE ATT&CK Matrix, the ATLAS Matrix shows the progression of adversarial tactics used in attacks specific to AI and NLP systems. This enables threat modelers to move from conceptual risk management issues to practical preventative and monitoring controls designed to protect models and training data.

Additional guidance and frameworks for AI & NLP systems can be found in:

- NIST's Report on Engineering Trustworthy Secure Systems (SP 800-160, Vol. 1, Rev. 1, 2022).
- NIST's Report on Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5, 2021).

Recommendations

- Developers and deployers of GenAI should review the frameworks and best practices referenced in this section, and implement the appropriate protocols to mitigate against cybersecurity threats.
- The task force recommends existing state statutes regarding cybersecurity should be amended to require that governmental organizations include specific and periodic testing for AI / NLP systems in risk assessments and vulnerability assessments.

Delivery of Public Services

While GenAI technologies promise enhanced efficiency, accessibility, and data-driven decision-making, their implementation in the public sector context raises pressing concerns about security, public trust, and ethical use. Governments face unique risks, including potential national security vulnerabilities, biases in decision-making, and increased dependency on proprietary technologies. The public's confidence in government services could erode if AI-driven systems fail to uphold transparency, fairness, and accountability.

Recognizing these risks is crucial as state and local governments explore GenAI applications to automate routine tasks, improve citizen engagement, and support critical services. With robust risk mitigation strategies and a focus on ethical AI governance, these tools can be responsibly leveraged to deliver meaningful benefits while safeguarding public trust and organizational integrity.

Potential Uses and Risks of GenAI

- Help process routine queries, provide timely responses, and help residents navigate government services like renewing licenses, accessing public records, and applying for benefits.
- Translate public materials into multiple languages and accessible formats (e.g., braille, audio) to ensure inclusivity for non-English speakers and individuals with disabilities.
- Process aerial and sensor data to assess damage, prioritize repairs, and allocate resources efficiently following public disasters.
- Can simulate environmental impacts and traffic patterns for infrastructure projects, recommending sustainable and efficient designs.

Governments are subject to specific risks related to the usage of AI and NLP. The integration of AI into local government critical infrastructure security can create a single point of failure if attacked or manipulated. Nation-state adversaries can leverage opportunities for backdoor or covert surveillance. Relying on proprietary AI platforms may also limit flexibility and increase costs.

Recommendations

Risk mitigation strategies for government entities must include the following aspects:

- Leverage secure AI governance frameworks by establishing clear policies for ethical GenAI use in public services and guidelines on transparency, accountability, and fairness, including incorporating principles such as "human in the loop" to mitigate against errors, bias, and overreliance on GenAI.
- Invest in state employees and domestic infrastructure to develop in-house GenAI capabilities and reduce reliance on foreign or proprietary technologies.

- Conduct initial and regular risk assessments to identify risks to the organization at the onset of a project and periodically throughout its lifecycle as GenAI capabilities (and risks) evolve quickly.
- Implement robust cybersecurity measures by hardening GenAI infrastructure with advanced security measures, such as adversarial training, secure APIs, and fraud detection routines.
- Establish clear and easy-to-use redress mechanisms for residents to challenge or appeal decisions made by AI and NLP-powered systems.
- Illinois must be explicit to its citizens about how AI is being used in government applications. Government must be held to the highest standards of accountability and transparency.

Conclusion

The Generative AI and Natural Language Processing Task Force convened during a pivotal moment as Illinois grappled with rapid advancements in artificial intelligence. The rise of Generative AI has already begun reshaping industries, education, and the workforce, while raising significant concerns about privacy, bias, and environmental impacts. Task force members, stakeholders, and subject-matter experts have collaborated over the past six months to analyze the opportunities and risks presented by this technology, identifying solutions that prioritize innovation while safeguarding public interest.

Throughout our discussions, it became clear that the integration of Generative AI into key sectors must be approached with deliberate policies, transparency, and accountability. This report represents the culmination of those efforts, offering a roadmap for policymakers to address immediate concerns while preparing Illinois for the long-term implications of Generative AI. By centering equity and ethical governance, the task force has focused on fostering responsible innovation that benefits all communities across the state.

A recurring theme throughout our work has been the importance of ensuring that the adoption of AI enhances – rather than diminishes – job quality, education, and civil liberties. The recommendations laid out in this report emphasize the need for collaboration among government, private industry, academic institutions, and civil society to navigate this evolving technological landscape. Addressing issues such as workforce training, consumer protection, and data privacy will require coordinated, forward-thinking policies and sustained efforts.

Illinois is a diverse state with a dynamic economy and a history of leadership in technology and innovation. The task force firmly believes that this report is a foundational step in positioning Illinois as a national leader in Generative AI governance. The next steps will include ongoing monitoring, evaluation, and refinement of policies, ensuring that Illinois remains proactive in addressing emerging challenges. The General Assembly should also carefully study additional policy areas that are being impacted by AI, including policing and public safety, healthcare, and insurance.

The work of this task force has been a testament to the power of collaboration and shared vision. By implementing the principles and recommendations outlined here, decision-makers can build an inclusive, ethical, and resilient framework for Generative AI. This approach will not only drive innovation but also safeguard the rights and well-being of all Illinois residents, ensuring a thriving workforce, an equitable society, and a future where technology serves the greater good.

Appendix A

1. While not exhaustive, the Council for Chief State School Officers collected state resources on AI[36]. So too, TeachAI[37] provides various resources germane to districts on AI policy. In recent weeks, the United States Department of Education's Office of Instructional Technology released a toolkit[38] for districts. This report is an extension/expansion of a previous report on AI and the future of teaching and learning also authored by the Office of Instructional Technology.
2. There is a wide range of foci for the collection, curation, and foci of AI resources that are applicable to schools and their work produced by organizations affiliated with institutions of higher education, policy, groups, and for profit companies (e.g., instructional supports[39], student learning[40], school and district operation[41], among others[42]). That this is so suggests the breadth of consideration AI requires in light of responsible implementation in the P-12 system as well as a means through which districts are provided a 'foothold' to easily and efficiently locate resources as they engage in their work.
3. Public Act 103-0451 and, in particular:
    - Model policies for schools to address AI use by students.
    - Model policies for schools to address use of AI in the classroom.
    - Protecting civil rights and civil liberties of individuals and consumers as it relates to AI.
    - Use of AI in the workforce and how this could affect employment levels, types of employment, and the deployment of workers.
    - Challenges of AI for cybersecurity.
4. Superintendents, for instance, when asked in a survey[43] administered nationally about AI and its use in teaching and learning and district and school operations, shared three views in tension with one another:
    4.1. Believe that AI is 'important and likely to impact'/is impacting the aforementioned,
    4.2. Do not feel prepared to lead their school system, and
    4.3. Among other pressures of the superintendency, do not see AI as an 'urgent' issue in 2024.
5. Work in the United Kingdom surveying[44] school personnel on topics of AI awareness, readiness, policies, professional learning, ethical use of AI, and chasm between student

[36] CCSSO. *Artificial Intelligence (AI) Resource Hub*.
[37] TeachAI (2024). *Foundational Policy Ideas for AI in Education.*
[38] U.S. Department of Education. *Artificial Intelligence and the Future of Teaching and Learning: Insights and Recommendations*.
[39] AI4K12 Initiative. *Building Capacity for K-12 Artificial Intelligence Education Research*.
[40] AI4K12 Initiative. *Grade Band Progression Charts.*
[41] Consortium for School Networking. (2023). *Artificial intelligence (AI) in K-12.*
[42] AI Education Project. *Are students ready for the age of artificial intelligence?*
[43] EAB. *2024 Voice of the Superintendent*
[44] Educate Ventures Research. (2024). *Shape of the Future: How education system leaders can respond to the provocation of artificial intelligence.*

awareness and use of AI outside of and while in school as well as a subsequent companion piece[45] suggests that there is an implementation gap between awareness of and readiness for the use of AI in classrooms, a lack of needed policies in place to bridge the aforementioned gap, and a need for professional learning on AI technology on account of the ever-emerging ethical issues inherent in the use of AI in schools.

6. The survey was issued to approximately 6700 IPA members and 1750 IASA members. This survey provided feedback from 219 school leaders (n=~3% response rate), with 96.8% from the public-school sector. There was a lack of representation from urban districts which represented just 5% of the data. While the response rate is too low to produce generalizations, of note is the range of perceptions between this survey and others shared in this report. Put differently, the wide range of perceptions, assumptions, and identified needs on account of these supports the subsequent recommendations in this report.
7. Note that the AI survey administered to IASA and IPA membership was modified from a benchmark tool[46] used in the development of the surveys referenced in Footnote 5.
8. There was a wide variance in the use of AI to generate instructional and/or operational resources, for instance, 85% of the respondents strongly disagreed, disagreed or somewhat agreed that teachers and administrators are using AI for these purposes.
9. Digital citizenship is the responsible use of technology by anyone who uses computers, the internet, and digital devices to engage with society on any level. It involves understanding and applying ethical principles, respecting others online, and protecting oneself from online threats (iCEV, 2023[47]).
10. Teach Plus, *Rules and Tools for AI-Powered Learning: Why Educators Can't Afford to Wait on AI Policies*
11. Digital Literacy is the ability to use information and communication technologies to find, evaluate, create, and communicate information. This involves both cognitive and technical skills. (American Library Association's Digital Literacy Task Force).

[45] Educate Ventures Research. (2024). *Beyond the Hype: The reality of AI in education across England.*
[46] https://www.educateventures.com/_files/ugd/c43582_e331aa3d5387431fb4ac531a33364dfb.pdf
[47] iCEV. (2024). *What Is Digital Citizenship & How Do You Teach It?*

Appendix B

Demographics:
Of the 219 respondents:

- 96.8% were employed in an Illinois public school,
- 58.9% identified as superintendents or employed at the district office,
- 34.7% principals, and 6.4% technologists,
- 73.1% respondents indicated they were employed at a Title 1 school,
- 54.8% worked in a rural community,
- 40.2% worked in a suburban community, and
- 5% worked in an urban area.

GenAI Awareness:

- 56.1% of the school leaders agreed or strongly agree that they possess a general understanding of the central concepts of GenAI.
- 24.2% agreed or strongly agreed that they possess a good understanding of how GenAI can be used in education.
- 9.1% agree or strongly agree that GenAI is being used to reduce teacher workload.[48]
- 62.6% of the respondents shared they do not believe GenAI is used to personalize student learning.
- 97.6% of school leaders lack confidence in how to use GenAI with students.
- 33.3% believe they understand the potential threats that GenAI poses to students.
- 8.2% strongly agree or agree that they understand how to develop safeguards against those threats.

Use of AI:

- 24.7% of school leaders believe their teachers are confident in how to use GenAI in the classroom setting.
- 79.5% shared concerns in their confidence of how to teach students to use GenAI appropriately.
- 6.8% of the respondents believe they have a clear approach in place for identifying and piloting tools that use GenAI.
- 80.8% do not use GenAI to support their learning at school.
- 65.8% shared they do not believe students are using GenAI at home to support their learning.
- 3.7% of those surveyed are confident that students are using GenAI tools appropriately.
- 9.1% have confidence that students are not using GenAI to generate explicit content or to create misinformation, hate speech, or cyberbullying.

[48] Appendix A.8

- 5% of those surveyed feel confident that students are not misplacing their trust in GenAI by sharing personal information or through unsupervised interactions, overreliance, bypassing restrictions, or by creating harmful content.

GenAI Policy and Leadership:

- 27.9% believe there is a strong appetite for AI amongst their leadership team.
- 9.1% have a clear approach in place for identifying and piloting AI tools.
- 65.3% of the respondents do not believe there is a leadership team or group at their school who is dedicated to coordinating the use of AI.
- 24.7% have a professional learning structure in place to address expertise and consistency in the understanding and use of AI.
- 11.4% of school leaders believe they are supporting students to use AI tools effectively, appropriately, and safely.
- 0% believe AI is being used to generate student feedback or mark student work.

Moreover, school leaders provided when asked if their school has an AI policy or strategy.

- 17.8% are not considering GenAI at this moment.
- 58.4% are considering GenAI, but do not have an GenAI policy or strategy.
- 16.9% are considering GenAI and have a policy or strategy.
- 6.8% are using GenAI and have a policy or strategy.
- 21.5% of the school leaders surveyed agreed that they have a policy for addressing GenAI threats or dangers.

When school leaders were queried on the employment of a digital citizenship[49] program across all grade levels to ensure students are prepared with the tools they need to use AI tools responsibly:

- 20.5% provided that either they do not implement a program and are not currently considering it.
- 37.9% do not currently implement a program but are presently considering doing so.
- 41.6% do implement a digital citizenship program.

AI Safety:

- 6.9% of those surveyed feel confident in allowing their pupils to use GenAI products.
- 16.9% believe there are guardrails in place to protect their students.
- 32.4% consider the forms/types of student data when choosing an GenAI platform.
- 47% identified they are confident in knowledge of and procedures for keeping a student's personal data safe.
- 25.6% of those surveyed considered how AI might impact equity at their school.

[49] Appendix A.9

- 29.2% are aware of the ways in which AI might show bias.
- 9.2% of school leaders believe that parents are aware of the AI products that their students interact with in the classroom setting.

Ethics:

- 5.5% of the school leaders who were surveyed expressed confidence in how they will measure and assess the impact AI has on students.
- 11.8% know the impact that they expect to achieve through the use of AI.
- 7.7% have clearly identified goals for technology in their schools.