



Interim Report

TO THE EIGHTY-NINTH TEXAS LEGISLATURE

HOUSE SELECT COMMITTEE ON ARTIFICIAL
INTELLIGENCE & EMERGING TECHNOLOGIES

MAY 2024

**HOUSE COMMITTEE ON ARTIFICIAL INTELLIGENCE & EMERGING
TECHNOLOGIES, SELECT
TEXAS HOUSE OF REPRESENTATIVES
INITIAL INTERIM REPORT 2024**

**A REPORT TO THE
HOUSE OF REPRESENTATIVES
89TH TEXAS LEGISLATURE**

**GIOVANNI CAPRIGLIONE
CHAIRMAN**

**COMMITTEE CLERK
KATY ALDREDGE**



Committee On
Artificial Intelligence & Emerging Technologies, Select

May 16, 2024

Giovanni Capriglione
Chairman


P.O. Box 2910
Austin, Texas 78768-2910

The Honorable Dade Phelan
Speaker, Texas House of Representatives
Members of the Texas House of Representatives
Texas State Capitol, Rm. 2W.13
Austin, Texas 78701


Dear Mr. Speaker and Fellow Members:

The Committee on Artificial Intelligence & Emerging Technologies, Select of the Eighty-eighth Legislature hereby submits its initial interim report for consideration by the Eighty-ninth Legislature.

Respectfully submitted,




Jeff Leach



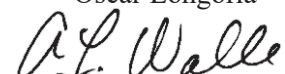
Angelia Orr



Giovanni Capriglione



Oscar Longoria



Armando Walle

TABLE OF CONTENTS

OVERVIEW	1
Charge	1
Introduction.....	1
Disclaimer	2
INTERIM STUDY TOPICS.....	5
TOPIC I: Background on Artificial Intelligence and Emerging Technologies	7
BACKGROUND	7
COMMITTEE ACTION.....	7
SUMMARY OF TESTIMONY	7
Background on AI: Testimony of Matthew Lease.....	7
Recommendations from Matthew Lease	14
TOPIC II: How Artificial Intelligence Affects Homeland & National Security	17
BACKGROUND	17
COMMITTEE ACTION.....	17
SUMMARY OF TESTIMONY	17
AI's Role in Defense: Testimony of Lieutenant General Richard Coffman	17
Recommendations from Lieutenant General Richard Coffman	20
AI's Role in Defense: Testimony of Lieutenant Steven Stone.....	21
Recommendations from Lieutenant Steven Stone.....	23
TOPIC III: How Artificial Intelligence Can Affect Elections	25
BACKGROUND	25
COMMITTEE ACTION.....	25
SUMMARY OF TESTIMONY	25
Impact of AI on Elections: Testimony of Nate Persily.....	25
Recommendations from Nate Persily	27
Impact of AI on Elections: Testimony of Samuel Derheimer	28
Recommendations from Samuel Derheimer	29
Impact of AI on Elections: Testimony of Andrew Cates.....	29
Recommendations from Andrew Cates	31
TOPIC IV: Dangers Presented by Artificial Intelligence	33
BACKGROUND	33
COMMITTEE ACTION.....	33
SUMMARY OF TESTIMONY	33
Dangers Presented by AI: Testimony of Lucas Hansen	33

Recommendations from Lucas Hansen	37
TOPIC V: The Intersection of Cybersecurity and Artificial Intelligence.....	39
BACKGROUND	39
COMMITTEE ACTION.....	39
SUMMARY OF TESTIMONY.....	39
Cybersecurity and AI: Testimony of Drew Hamilton.....	39
Recommendations from Drew Hamilton	42
TOPIC VI: Comparing Industry and Advocacy Perspectives	43
BACKGROUND	43
COMMITTEE ACTION.....	43
SUMMARY OF TESTIMONY.....	43
Comparing Industry and Advocacy Perspectives: Testimony of Renzo Soto	43
Recommendations from Renzo Soto	44
Comparing Industry and Advocacy Perspectives: Testimony by Justin Brookman.....	45
Recommendations from Justin Brookman.....	46
Comparing Industry and Advocacy Perspectives: Testimony of Matthew Scherer	47
Recommendations from Matthew Scherer.....	47
Comparing Industry and Advocacy Perspectives: Testimony of Kevin Welch	47
Recommendations from Kevin Welch.....	48
CONCLUSION.....	49
ENDNOTES	50

OVERVIEW

Charge

By proclamation dated April 2, 2024, Dade Phelan, Speaker of the House of Representatives, formed the House Select Committee on Artificial Intelligence & Emerging Technologies.

The committee was created to conduct a comprehensive review of the advancements in artificial intelligence and emerging technologies (AI/ET) and the economic, ethical, and societal implications of those advancements. The review includes:

1. Examining the current state of AI/ET and its uses by public and private actors in modern society;
2. Determining the impact of the application of AI/ET on various sectors of society, including employment, healthcare, homeland and national security, and transportation;
3. Identifying policy considerations necessary to ensure the responsible deployment of AI/ET in Texas by both public and private actors; and
4. Formulating recommendations for legislative, policy, regulatory, and remedial actions needed to address the challenges and opportunities presented by AI/ET.

The committee was directed to submit an initial report no later than May 16, 2024, in the same manner as an interim study committee under Rule 4, Section 61, Rules of the House of Representatives.

Introduction

The Select Committee on Artificial Intelligence and Emerging Technologies met on April 29, 2024 to hold an initial hearing to receive a broad overview of artificial intelligence and emerging technologies. The committee heard from a comprehensive range of witnesses to provide an introduction to AI covering the following topics:

- How AI affects the military;
- Why AI is making the prosecution of child pornography laws difficult,
- How AI can impact elections;
- How AI is making cybersecurity both more efficient and more problematic; and
- A comparison of how industry and advocacy associations differ in their arguments.

This initial interim report is only intended to give an overview of the testimony the committee heard. It is the committee's hope that such testimony will illuminate the basic principles around artificial intelligence and emerging technologies while also drawing attention to both its stunning potential and frightening drawbacks. In addition to providing detailed summaries of the testimony, the report relays for broad consideration a number of policy recommendations offered by each witness.

The committee intends to continue exploring issues related to its charge in subsequent hearings and reports. This initial report's purpose is to provide a basic foundation from which to launch into more detailed and in-depth discussions. This seemingly boundless new frontier is evolving in

real-time. There is much to tackle and even more to learn. Accordingly, any viewpoint or recommendation's presence in this report does not signify endorsement. Instead, they provide inspiration for thought and offer a glimpse into potential ideas or avenues to achieve the committee's ultimate goal.

Emerging technology and AI are developing at a breakneck pace; it is not an exaggeration to say it changes by the day. Its impact on society will be profound, but it is also dangerous. Therefore, it is incumbent upon us as a legislative body to be knowledgeable if we are to simultaneously embrace the good while warding off the bad. Armed with knowledge, we can accomplish our goal: to produce a fair, ethical, and practical framework to be used by the Texas Legislature and other regulatory and policy bodies to address the implications of this revolutionary and ostensibly supernatural technology.

The definition of artificial intelligence has evolved over time. The definition currently in Texas statute was originally taken from the 2019 European Union High-Level Expert Group on Artificial Intelligence and is found in many early-state AI laws. Sec. 2054.621(2), Government Code defines an artificial intelligence system as a system capable of:

- (A) perceiving an environment through data acquisition and processing and interpreting the derived information to take an action or actions or to imitate intelligent behavior given by a specific goal; and
- (B) learning and adapting behavior by analyzing how the environment is affected by prior actions.”

In 2023, the European Union chose to adopt a more updated definition that more recent state-level laws have preferred. The updated definition as defined by the Organisation for Economic Co-operation and Development (OECD) is, “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. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.” The OECD Policy Principles on Artificial Intelligence have been formally adopted by 42 nations, including the United States and all G-20 countries.

Disclaimer

This report, crafted by the House Select Committee on Artificial Intelligence and Emerging Technologies, leverages a spectrum of AI tools to enhance the production process. AI voice cloning models, created using publicly available audio of each committee member, presented the introductory remarks. After posting the committee video, an audio extractor was used to rip the audio from the 5 1/2 hour hearing. This audio was then uploaded to a machine learning-based service that converted the audio to text. The resulting transcripts include detailed metadata, such as confidence scores and timestamps for each word and punctuation mark. The text was segmented and processed by a large language model, which performed summarization, created a table of contents, facilitated research across diverse subjects, and streamlined the organization of written testimonies. Further queries were used to extract the most impactful quotes from the witnesses and highlight key recommendations.

While AI played a role in augmenting the efficiency of the production process, it is important to acknowledge that much of the work, including research, editing, proofreading, and content refinement, was conducted by human writers, researchers, and editors. Thus, readers are encouraged to interpret the contents of this report within the context of its collaborative creation, blending the capabilities of AI with human expertise.

It is important to note that no private or confidential information was shared with any LLM tools during the development of this report.

INTERIM STUDY TOPICS

- TOPIC I:** Background on Artificial Intelligence and Emerging Technologies
- TOPIC II:** How Artificial Intelligence Affects Homeland & National Security
- TOPIC III:** How Artificial Intelligence Can Affect Elections
- TOPIC IV:** Dangers Presented by Artificial Intelligence
- TOPIC V:** The Intersection of Cybersecurity and Artificial Intelligence
- TOPIC VI:** Comparing Industry and Advocacy Perspectives

TOPIC I: Background on Artificial Intelligence and Emerging Technologies

BACKGROUND

Artificial intelligence is transforming our world, offering unprecedented opportunities but also presenting new challenges. To understand how artificial intelligence has developed, the committee invited Matthew Lease, a subject matter expert to provide background on the technology's advancements. Professor Lease is a Professor of Information and Computer Science at the University of Texas at Austin, a *Distinguished Member* of the Association for Computing Machinery (ACM) and a *Senior Member* of the Association for the Advancement of Artificial Intelligence (AAAI).

COMMITTEE ACTION

Public Hearing: April 29, 2024 – Austin, Texas, Capitol Extension E2.026, at 10:00 a.m.

Witness Testimony:

- Matthew Lease, Professor, University of Texas at Austin School of Information

SUMMARY OF TESTIMONY

Background on AI: Testimony of Matthew Lease

The widespread nature of AI has high-profile uses along with everyday applications. Generative AI can capture public attention by producing fictitious text and images like, in an example shared by Professor Lease, a picture celebrating a fictional, 2024 Dallas Cowboys Super Bowl win. Despite these headline-grabbing cases, Professor Lease stressed that AI's integration into the fabric of everyday life is far more extensive and mundane, encompassing technologies such as traffic navigation, spam filters, and systems that give recommendations for movies and shopping. With the advancements in technology, AI has even played a role in automated evaluation systems used in testing, including in the use of grading written portions of standardized testing.

With the good, comes the bad, and risks associated with AI must be acknowledged. Professor Lease provided several examples of AI-induced issues like the misuse of AI in creating deceptive images of celebrities or explosive events, which can disrupt public peace and affect stock markets. He recalled the 2010 "flash crash," a type of stock market crash triggered by selling pressure from the sell algorithm, pointing out the longstanding history of AI's impact on society. Professor Lease noted that "there will never be a time when AI never has a crash in a self-driving car. The question we should be thinking about is when it would have fewer crashes than people do right now today because that's a chance for us to start saving lives." In light of this, many tech companies are already implementing guardrails to ensure responsible AI use because they ultimately want to be both successful and safe. A new framework by the National Institute of Standards and Technology (NIST) recently released¹ an AI Risk Management Framework that provides a list of potential risks with Gen-AI:

-
1. CBRN Information: Lowered barriers to entry or eased access to materially nefarious information related to chemical, biological, radiological, or nuclear (CBRN) weapons, or other dangerous biological materials.
 2. Confabulation: The production of confidently stated but erroneous or false content (known colloquially as “hallucinations” or “fabrications”).
 3. Dangerous or Violent Recommendations: Eased production of and access to violent, inciting, radicalizing, or threatening content as well as recommendations to carry out self-harm or conduct criminal or otherwise illegal activities.
 4. Data Privacy: Leakage and unauthorized disclosure or de-anonymization of biometric, health, location, personally identifiable, or other sensitive data.
 5. Environmental: Impacts due to high resource utilization in training GAI models, and related outcomes that may result in damage to ecosystems.
 6. Human-AI Configuration: Arrangement or interaction of humans and AI systems which can result in algorithmic aversion, automation bias or over-reliance, misalignment or misspecification of goals and/or desired outcomes, deceptive or obfuscating behaviors by AI systems based on programming or anticipated human validation, anthropomorphization, or emotional entanglement between humans and GAI systems; or abuse, misuse, and unsafe repurposing by humans.
 7. Information Integrity: Lowered barrier to entry to generate and support the exchange and consumption of content which may not be vetted, may not distinguish fact from opinion or acknowledge uncertainties, or could be leveraged for large-scale dis- and misinformation campaigns.
 8. Information Security: Lowered barriers for offensive cyber capabilities, including ease of security attacks, hacking, malware, phishing, and offensive cyber operations through accelerated automated discovery and exploitation of vulnerabilities; increased available attack surface for targeted cyber attacks, which may compromise the confidentiality and integrity of model weights, code, training data, and outputs.
 9. Intellectual Property: Eased production of alleged copyrighted, trademarked, or licensed content used without authorization and/or in an infringing manner; eased exposure to trade secrets; or plagiarism or replication with related economic or ethical impacts.
 10. Obscene, Degrading, and/or Abusive Content: Eased production of and access to obscene, degrading, and/or abusive imagery, including synthetic child sexual abuse material (CSAM), and nonconsensual intimate images (NCII) of adults.
 11. Toxicity, Bias, and Homogenization: Difficulty controlling public exposure to toxic or hate speech, disparaging or stereotyping content; reduced performance for certain sub-groups or languages other than English due to non-representative inputs; undesired homogeneity in data inputs and outputs resulting in degraded quality of outputs.
 12. Value Chain and Component Integration: Non-transparent or untraceable integration of upstream third-party components, including data that has been improperly obtained or not cleaned due to increased automation from GAI; improper supplier vetting across the AI lifecycle; or other issues that diminish transparency or accountability for downstream users

The Redefining of AI

Artificial intelligence, as a field, originated in 1956, although the applications and concepts predate this. Professor Lease explained, “[w]e keep moving the goalposts for what we call AI.” This is known as the “AI effect,” where successful AI applications become so integrated and commonplace that they are no longer recognized as AI—a phenomenon that leads to a continuous redefinition of the term. He used the example of early 20th-century ‘computers’—people who performed calculations by hand—that were replaced by mechanical calculators, now a mundane technology not considered AI. This shift reflects the broader trend of AI becoming an invisible part of technology once it becomes fully assimilated into everyday use.

AI Outputs and Autonomy Spectrum

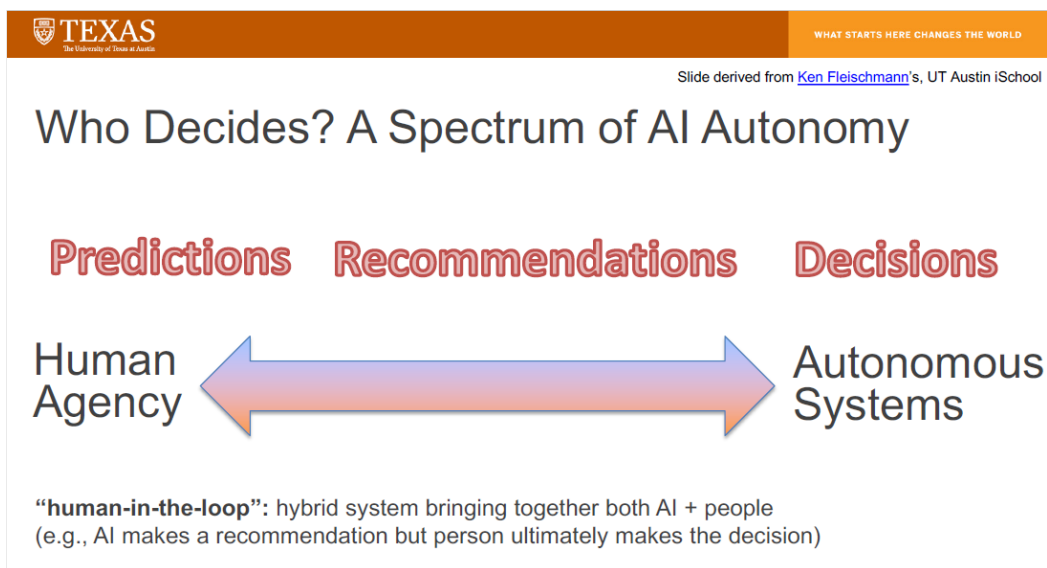


Figure 1. The Spectrum of AI Autonomy (provided by Matthew Lease)

The spectrum of AI autonomy defines how AI’s role ranges from passive information provider to active decision-maker and underscores the varied implications of each level of autonomy in terms of user control and trust in AI systems. The functionalities of AI can be categorized by its outputs into three types, each category representing a different level of AI autonomy:

- **Predictions**
Predictive AI might forecast the weather, leaving the user to decide how to use this information.
- **Recommendations**
Recommender systems suggest products or media, influencing user choices but ultimately leaving the decision to them.

- Decisions

Decision-making AI, like spam filters or autonomous vehicles, act independently based on its programming.

Evolution of AI and AI Hype Cycles

Professor Lease explained, “The field of AI has twice undergone major ‘hype’ cycles of unrealistic expectations, followed by significant drops in interest and investment.” He noted that after periods of intense excitement and inflated expectations about AI's capabilities, there typically follows a phase of disappointment when these expectations are not met, leading to what is known as an "AI winter." It is possible that today's excessive hype could again lead to disillusionment.

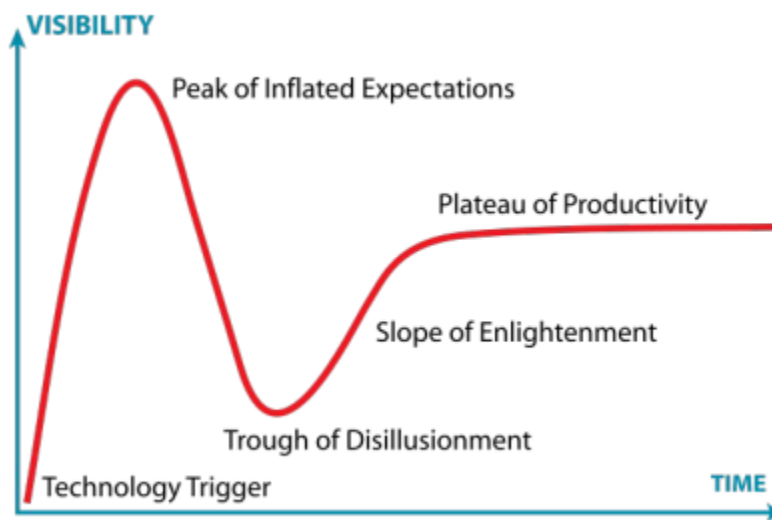


Figure 2. AI Winter

Expert Systems created in the 1970s and 1980s failed due to their inability to handle complex, nuanced decisions. These systems started by asking human experts (e.g. doctors) how they would make a decision in different scenarios, then encode their answer as “if-then” rules for the system. The transition to modern machine learning techniques allowed AI to learn and identify patterns from data without explicit programming for each specific task. AI has now become increasingly data-driven, particularly through machine learning and deep learning. Machine learning algorithms detect patterns in large data sets and learn to make predictions by processing data, rather than receiving explicit programming instructions. Deep learning uses neural networks, inspired by the way neurons interact in the human brain, to ingest data and process it through multiple iterations that learn increasingly complex features of the data and make increasingly sophisticated predictions. Modern AI systems, such as spam filters or recommendation engines, learn from vast amounts of data to make predictions or decisions, improving as they access more data.

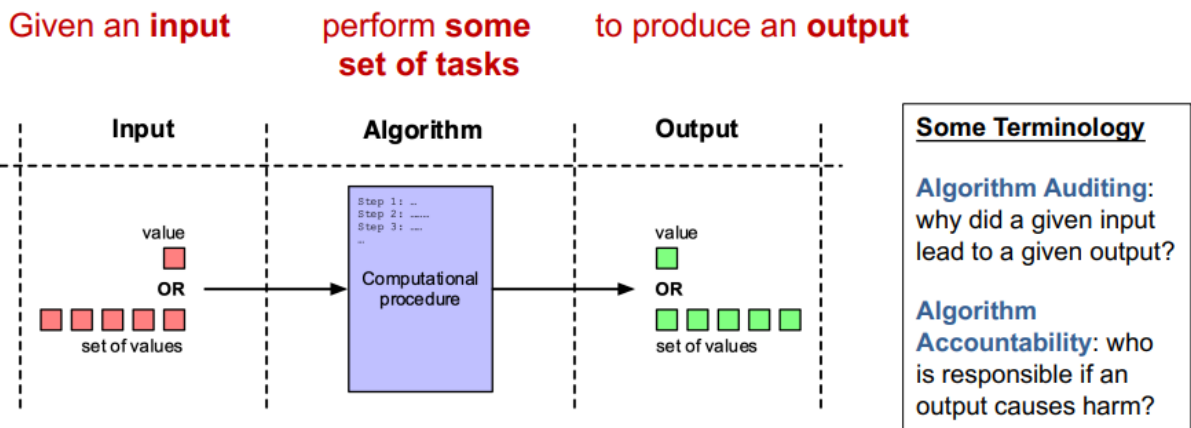


Figure 3. What is an Algorithm

The Importance of Data Quality

While data quantity enhances AI performance, data quality is critical, as poor-quality data can lead AI to reinforce existing biases or produce errors. “If you train AI on low-quality data, it will yield low-quality AI,” Professor Lease warned. Generative AI can sometimes “hallucinate” or create false information based on the biases or inaccuracies in the training data. Training AI on high-quality, curated data to significantly reduce errors and biases is important. Using well-chosen data can enhance AI learning efficiency by focusing on high-quality input rather than merely increasing the volume of training data.

It is important to align AI outputs with human values and oversight, especially in sensitive applications. Professor Lease introduced the concept of supervised versus unsupervised learning, where supervised learning involves AI learning from labeled data to perform specific tasks, while unsupervised learning involves AI identifying patterns without specific guidance. This distinction is crucial for developing AI systems that are both effective and ethical, minimizing the risk of perpetuating biases or making inaccurate predictions.

AI transparency is critical, and we need mechanisms to understand and audit AI decisions, which is referred to as the “black box” problem. Transparency is crucial for trust and accountability, especially when AI is used in decision-making processes that can significantly impact people’s lives. Professor Lease emphasized that as AI systems grow more complex, the ability of even their creators to understand their function diminishes, necessitating increased efforts toward making AI operations more interpretable and explainable.

The role of stakeholders in enforcing AI transparency and fairness is essential. Professor Lease suggested that legislatures could require disclosures about the data used to train AI systems, ensuring that users understand the basis on which AI makes decisions. This transparency would build trust and allow users to make informed decisions about relying on AI outputs.

Enhancing AI Governance and Addressing Disinformation

According to Professor Lease, robust governance frameworks are needed to ensure fairness, reliability, privacy, transparency, sustainability, and accountability in AI applications. This is also

known as “Responsible AI.” It is important to have governance and responsibility both within organizations and in broad public policy contexts. There could be challenges around privacy and security, especially concerning data collected without clear consent, which could be exploited or misused.

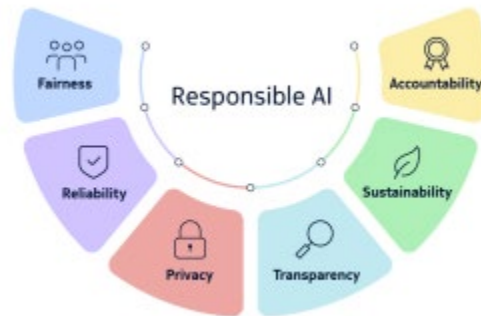


Figure 4. AI Governance Structure

In his discussion regarding AI's role in the creation and spread of misinformation, particularly in elections, Professor Lease pointed out the critical need for "human-in-the-loop" systems to effectively review AI outputs, and manage and mitigate the proliferation of false information. He described ongoing public and private efforts to improve AI governance, with initiatives like the Good Systems initiative. This project at the University of Texas is aimed at ensuring AI technologies reflect societal values and minimize harm, underscoring the importance of diverse perspectives in developing responsible AI frameworks. Good AI governance involves ensuring that AI systems do not disproportionately affect vulnerable groups and maintaining high standards of information integrity to protect against misinformation. This is especially necessary during elections.

AI “black boxes” are created when decisions made by an AI system are made in an opaque way that humans, even the system developers themselves, do not easily understand. Thus it is difficult to understand how an AI system arrives at its conclusion or prediction. Professor Lease stressed the need for greater transparency and interpretability in AI to build trust in the systems and allow users to understand and verify AI decisions.

Addressing AI Bias and Data Representation Challenges

Another crucial aspect of AI governance is the importance of addressing bias in AI applications. He highlighted the risk of AI perpetuating existing social biases, particularly through the data on which it is trained. If an AI model is trained on biased data the results will reflect that. AI developers must intentionally select diverse and representative data sets to train AI systems, ensuring they function equitably across different populations and scenarios.

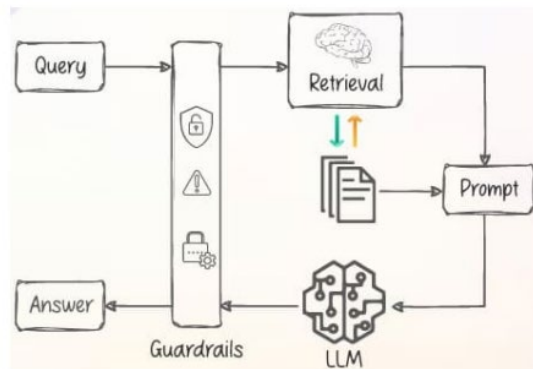


Figure 5. Guardrails Difficult to Implement

Rural areas with limited internet access also present technological and operational challenges as they may not be adequately represented in the data AI models are trained on. This further underscores the need for careful consideration of data sources and training methods in AI development.

Professor Lease advocated for proactive measures in AI governance to prevent and address issues before they arise rather than reacting to problems after they have caused harm. This proactive approach is essential to ensure that AI technologies are developed and implemented in ethical, equitable, and beneficial ways.

Selecting and processing data for AI models is complicated. Professor Lease highlighted the challenges of ensuring data quality and equal representation, both of which are critical for training reliable AI systems. Biases exist that can be introduced during the data collection and labeling processes, where subjective judgments by human annotators can significantly influence AI behavior. Several challenges exist in the collection and labeling process of the data needed to train AI models; the computer technology company Oracle lists several in the figure below:

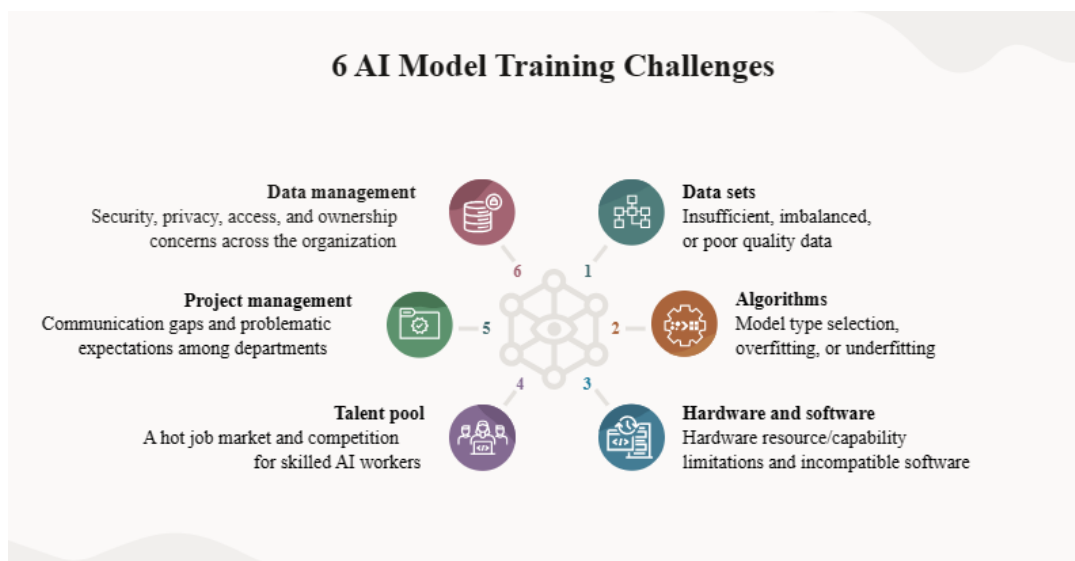


Figure 6. AI Model Training Challenges

Professor Lease emphasized the importance of diversity in both the data used and the teams handling it to prevent biases and ensure fair outcomes across different demographics. “The world is a biased place, and the data on the web training an AI program is biased. We need to be intentional and thoughtful about data collection and ensuring diverse representation,” Professor lease summarized. He explained that even well-intentioned AI systems can perpetuate existing societal biases if the data they learn from is not carefully curated and balanced. This requires thoughtful consideration of where data is sourced, how it is labeled, and the diversity of perspectives included in its processing and analysis.

AI Influence on Consumer Behavior and Data Handling Challenges

In discussing the significant impact of AI on consumer behavior, particularly through recommendation systems used by online platforms, Professor Lease explained that these systems guide users toward certain products. That guidance could be based on a specific data set collected from their own and similar others' behaviors. This can limit exposure to a broad range of options and instead lead to a narrowing of choices, effectively shaping their purchasing and browsing habits.

Professor Lease also touched on the future of physical retail, which he predicts will increasingly integrate digital technologies, such as facial recognition and targeted digital advertising, blurring the lines between online and in-store shopping experiences. This integration suggests a future where digital and physical retail environments influence consumer behavior through sophisticated and pervasive AI technologies. Several models already exist in this arena². The grocery chain Kroger has acquired a company to help optimize variable pricing by applying predictive behavior modeling to segment shoppers and create individualized experiences, including personalized promotions and tailored pricing. Ahold Delhaize, a Dutch Retailer has implemented a blockchain AI solution to trace the origin of their private label products, and Trigo, a computer vision AI company solving retail challenges including loss prevention and theft, has partnered with grocery chains Tesco and Aldi to provide grab-and-go technology which scans items automatically using AI computer vision.

Recommendations from Matthew Lease

- **Transparency and Data Provenance:** Implement requirements for AI models to disclose the data sources they use for training. This could help in ensuring that the data driving AI decisions is reliable and ethically gathered.
- **Quality of Data:** Emphasize the importance of high-quality data in AI training processes to avoid biases and enhance the reliability of AI outputs.
- **Human Oversight:** Encourage the implementation of 'human-in-the-loop' systems to ensure that AI does not operate entirely autonomously, particularly in critical decision-making processes.
- **Bias and Fairness:** Consider how AI might perpetuate existing societal biases and explore ways to mitigate this, such as using diverse data sets and teams to develop and train AI systems.
- **Privacy and Security:** Weigh the implications of AI on personal privacy and data security, considering how AI can be used to enhance or undermine these aspects.

-
- Educational Initiatives: Develop educational programs that could prepare the workforce for the evolving demands of an AI-driven economy.
 - Regulatory Frameworks: Outline the need for comprehensive regulatory frameworks that address the ethical, legal, and social implications of AI.
 - Cross-Sector Collaboration: Advocate for partnerships between academic institutions, industry, and government to foster socially responsible and beneficial innovations in AI.

TOPIC II: How Artificial Intelligence Affects Homeland & National Security

BACKGROUND

Artificial intelligence holds significant promise and challenges for homeland and national security. We have seen the integration of AI into modern warfare and public safety, offering capabilities that range from vision and sensing to language generation and data analysis. However, its deployment raises ethical, legal, and strategic questions regarding autonomy, accountability, and privacy.

COMMITTEE ACTION

Public Hearing: April 29, 2024 – Austin, Texas, Capitol Extension E2.026, at 10:00 a.m.

Witness Testimony:

- Lieutenant General Richard Coffman, Deputy Commanding General, Army Futures Command
- Lieutenant Steven Stone, IIS CITEC Staff Captain, Department of Public Safety

SUMMARY OF TESTIMONY

AI's Role in Defense: Testimony of Lieutenant General Richard Coffman

Lieutenant General Richard Coffman, representing the United States Army, testified as to the importance and complexity of artificial intelligence within the defense sector. First introduced in the military 40 years ago to create missile targeting systems, AI technology has rapidly evolved. Powered by advanced chips and extensive data, today it encompasses a wide range of capabilities, from language generation to real-time data analysis. Notably, AI is used to make better decisions based on real-time data. We can now target adversaries by combining different vantage points from the air and ground to create an advantage or use computer vision, a type of AI that uses images and videos to identify and understand objects, to determine facilities, movement, people, and animals to help determine if action is acceptable under the rules of war.

In a military context, AI enhances decision-making, provides a relative advantage on the battlefield, and optimizes resource allocation in public safety scenarios, despite its imperfections and potential biases. Applications include target identification, assessment of collateral damage, detection of chemical weapons outbreaks, managing the load on power grids, and critical infrastructure protection.

The ethical use of AI is crucial for ensuring compliance with international laws, rules of engagement, and the targeting of adversaries. Human oversight is imperative to prevent AI systems from operating autonomously and making decisions beyond established parameters. Lt. Gen. Coffman observed that many countries use AI to develop models that will be blindly followed. However, he advocated for a framework where artificial intelligence systems are never fully autonomous within our military and security communities. Instead, these systems should

function strictly within human-defined guidelines, in the same vein as “human-in-the-loop” systems reviewing the output of the AI creation.

For instance, the International Committee of the Red Cross recently made urgent appeals to global organizations, proposing bans on autonomous weapons. They highlighted the immediate humanitarian concerns posed by such technologies, stating, "Autonomous weapons are not mere science fiction from a distant dystopian future; they are a pressing concern that necessitates an urgent international political response." The Red Cross committee further noted that, "Increasingly, weapons are being developed and deployed — in the air, on land, and at sea — that select and engage targets without human intervention."

Concerns about bias, privacy infringement, and the potential for disinformation and deep fakes underscore the need for clear regulations and accountability measures. While we can acknowledge AI's potential to improve battlefield logistics and strategy, Lt. Gen. Coffman stressed the persistent need for ethical considerations, particularly regarding autonomous weapons systems. He firmly stated the U.S. Army's stance on keeping humans in the loop to prevent fully autonomous decision-making in combat, reflecting a commitment to ethical warfare. Additionally, there is concern about an “invisible battlefield,” like cyber warfare and information warfare. If our adversaries use technology for bad, will that deter air, ground, and sea combat? What leader would send troops into battle if they knew the likelihood was mutually assured destruction?

AI's Impact on Public Safety and Infrastructure

Lt. Gen. Coffman discussed AI's applications in public safety and infrastructure management, highlighting how AI enhances predictive analyses to manage everything from emergency services to power grids. This capability is vital for planning and response, potentially transforming how services are delivered and crises are managed. In 20 years, the predictive models will foresee supply chain needs, such as ramping up production at an ammunition plant because of imminent demand.

However, all of this technological advancement and the use of data come with dangers. Lt. Gen. Coffman expressed concerns about data privacy and security, especially in light of AI's capability to process vast amounts of personal and sensitive information. He called for robust governance measures to protect privacy and ensure the security of data used in AI systems.

The National Security Guidance, Defense Governance, and Future Outlook

Lt. Gen. Coffman advocated for continuous education on AI capabilities and limitations to mitigate risks associated with misinformation and data manipulation. This educational focus is crucial for both the public and decision-makers to navigate the evolving landscape of AI and its applications. He cautioned against complacency, urging ongoing investment in AI research and development to maintain a technological edge over potential adversaries.

Last year, the Biden Administration released Executive Order 14110, which detailed significant directives for the Department of Defense (DoD), including:

-
- Development and Implementation of Safety Measures
 - The DoD is tasked with developing and implementing plans to use AI to evaluate and mitigate security risks. This includes developing AI model evaluation tools and testbeds to understand and mitigate these risks.
 - Reporting Requirements for a Dual-Use AI Model
 - Companies developing or intending to develop dual-use AI models are required to report to the government on model training, testing, and data ownership. The DoD is one of the agencies involved in defining the technical conditions that determine which models and computing infrastructures are subject to this reporting.
 - Biosecurity and National Security
 - The DoD is also responsible for studying and reporting on the use of AI in biology and its potential to increase biosecurity and national security risks, as well as making recommendations to mitigate such risks.
 - Chemical, Biological, Radiological, and Nuclear (CBRN) Threats
 - The Department of Homeland Security (DHS), in coordination with the DoD and other agencies, is tasked with evaluating the potential for AI to be used to develop, produce, or counter CBRN threats.

DoD's Five Principles for the Ethical Use of AI:

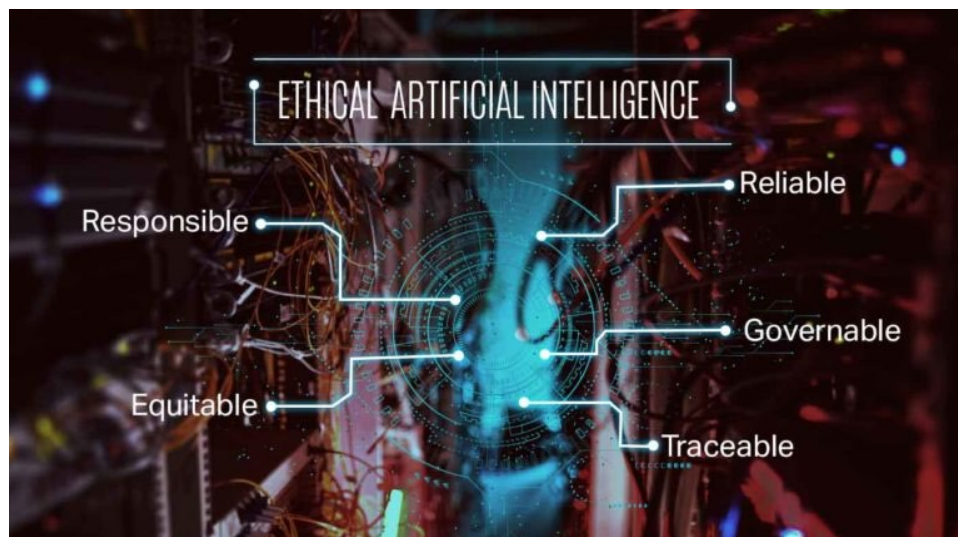


Figure 7. Ethical Artificial Intelligence

The DoD introduced five principals for the ethical use of AI applied to both combat and non-combat functions:

- Responsible
 - DoD personnel will exercise appropriate levels of judgment and care while remaining responsible for the development, deployment, and use of AI capabilities.

-
- Equitable
 - DoD will take deliberate steps to minimize unintended bias in AI capabilities.
 - Traceable
 - DoD’s AI capabilities will be developed and deployed such that relevant personnel possess an appropriate understanding of the technology, development processes, and operational methods applicable to AI capabilities, including with transparent and auditable methodologies, data sources, and design procedure and documentation.
 - Reliable
 - DoD’s AI capabilities will have explicit, well-defined uses, and the safety, security, and effectiveness of such capabilities will be subject to testing and assurance within those defined uses across their entire life-cycles.
 - Governable
 - DoD will design and engineer AI capabilities to fulfill their intended functions while possessing the ability to detect and avoid unintended consequences, and the ability to disengage or deactivate deployed systems that demonstrate unintended behavior.

AI’s Role in National Security

In March 2024, the U.S. Army released a 100-day plan to quickly identify all obstacles to adopting AI. The Army recognized that private industry would be better suited to design algorithms and develop models. The plan's goal is to examine every obstacle and prepare for the risks of AI. Recently, the National Security Agency created³ a new entity to oversee the development and integration of AI capabilities within U.S. national security systems. The seriousness with which AI is being considered underscores the global efforts around AI as a national security issue.

Lt. Gen. Coffman's testimony stressed the critical balance between quickly leveraging AI for its vast capabilities, in and outside of the U.S. military's use, and instituting stringent controls to safeguard ethical standards and human welfare. This balance is essential as AI continues to permeate all aspects of society, from military operations to public safety and beyond.

Recommendations from Lieutenant General Richard Coffman

- Education on AI: Educate the public, especially the youth, about what is real and what is not in the domain of AI to prevent misinformation and misinterpretations.
- Research and Academic Partnerships: Develop and strengthen partnerships between federal and state entities and academic institutions to enhance AI research and applications, particularly in public safety and defense.
- Privacy and Security Policies: Advocate for the creation of state and federal policies that protect individuals' privacy and secure personal and public data against cyber threats.

-
- **Accountability for Nefarious Actions:** Establish clear guidelines and laws that hold individuals and entities accountable for misuse of AI, particularly in contexts that threaten public safety or involve disinformation.
 - **Human Oversight in AI Application:** Acknowledge the imperfections of AI models and the necessity for continuous human involvement to monitor AI performance and adjust confidence levels in AI decisions.
 - **Ethical Use of AI in Military and Public Safety:** Maintain strict ethical standards in the deployment of AI, particularly in sensitive areas like military operations and public safety, ensuring AI acts within the constraints of clearly defined rules.
 - **Integrate AI with Human Decision-Making:** Utilize AI to enhance decision-making in military strategies by providing comprehensive real-time data but ensure the final decisions are made or reviewed by humans.
 - **Robustness Against AI Spoofing and Errors:** Increase efforts to train and retrain AI algorithms using both real and synthetic data (data that is created using generative AI) to minimize errors and enhance the reliability of AI applications in critical operations.

AI's Role in Defense: Testimony of Lieutenant Steven Stone

Lieutenant Steven Stone of the Texas Department of Public Safety discussed AI's dual role in law enforcement, highlighting its benefits and challenges. Lt. Stone, who specializes in cybercrime and digital forensics, underscored how AI aids in analyzing vast amounts of data, categorizing images, and identifying trends in criminal activities. Notably, he pointed out AI's effectiveness in identifying victims of child sexual abuse by recognizing patterns in visual data, such as specific objects present in the background of videos or photos.

However, Lt. Stone also addressed the significant challenges posed by AI, particularly in how the technology complicates existing legal frameworks. He explained that while AI can enhance the identification of illicit materials, such as child pornography, the laws have not kept pace with technology, especially regarding AI-generated content. This gap presents significant difficulties in prosecuting cases where the victims cannot be identified or where AI creates realistic but non-real depictions of abuse, thus complicating the legal process.

The National Center for Missing and Exploited Children (NCMEC) released a report⁴ stating that there was an alarming increase in reports involving generative AI (GAI), artificial intelligence capable of generating text, images, videos, or other data using generative models in response to prompts. In 2023, the CyberTipline, a centralized reporting system for the online exploitation of children operated by NCMEC, received 4,700 reports of Child Sexual Abuse Material (CSAM) or other sexually exploitative content related to generative AI⁵. GAI CSAM portrays computer-generated children in graphic sexual acts and can be generated at will by the user of certain GAI platforms. GAI can also be utilized to create deepfake sexually explicit images and videos by using an innocent photograph of a real child to create a computer-generated one. Examples seen by NCMEC include actual prompts entered into dark web AI models describing graphic requests to generate child sexual abuse material.

In addition, a recent FBI Public Service Announcement⁶ gave examples of cases involving

individuals having altered images into CSAM. These include a child psychiatrist and a convicted sex offender. In November 2023, a child psychiatrist in Charlotte, North Carolina, was sentenced to 40 years in prison, followed by 30 years of supervised release, for sexual exploitation of a minor and using GAI to create CSAM images of minors. Regarding the use of AI, the evidence showed the psychiatrist used a web-based GAI application to alter images of actual, clothed minors into CSAM. Also in November 2023, a federal jury convicted a Pittsburgh, Pennsylvania, registered sex offender of possessing modified CSAM of child celebrities. The Pittsburgh man possessed pictures that digitally superimposed the faces of child actors onto nude bodies and bodies engaged in sex acts. There were also incidents of teenagers using AI technology to create CSAM by altering ordinary clothed pictures of their classmates to make them appear nude.

Legal Challenges and AI in Law Enforcement

Lt. Stone further detailed the specific legal challenges law enforcement faces with the advent of AI technologies. Current child pornography laws address AI to an extent, but they require that law enforcement identify a known victim or have a victim of whom AI-generated material is in the likeness of. “With AI technology today, we may never know who that victim is,” explained Lt. Stone. With the proliferation of AI image generators, it has become easier for the average person to generate an image of a child that has no likeness to a known child. Therefore, the creation of that image cannot be prosecuted.

Relevant Portion of Title 9 Sec. 43.26.

For purposes of conduct prohibited under this section, visual material to which that conduct applies includes a depiction of a child:

- (1) who is recognizable as an actual person by the person’s face, likeness, or other distinguishing characteristic, such as a unique birthmark or other recognizable feature; and**
- (2) whose image as a child younger than 18 years of age was used in creating, adapting, or modifying the visual material, including computer-generated visual material that was created, adapted, or modified using an artificial intelligence application or other computer software.

Lt. Stone highlighted the use of "deep fakes" and AI-generated images in criminal activities to stress the need for updated laws that better address such technologies' nuances. Current laws only allow prosecution if videos are sexual in nature. Still images are not addressed. Lt. Stone pointed out that current regulations are often inadequate for handling cases involving AI-generated content because it does not fit neatly into existing legal definitions of criminal activity.

Furthermore, Lt. Stone discussed the escalation in scams facilitated by AI, such as those involving synthetic voice technologies that could trick victims by mimicking the voices of their loved ones. “The ability to mimic someone’s voice with very few words is increasing and becoming easier,” Lieutenant Stone testified. This evolving threat landscape calls for more sophisticated consumer education and legal frameworks to protect individuals from such technologically advanced frauds. In his concluding remarks, Lt. Stone called for a proactive legislative response to the challenges

posed by AI in public safety. He advocated for laws that are flexible enough to address AI's rapidly evolving capabilities, including provisions to handle cases of AI-generated child and adult pornography. "If the intent of the possession of child pornography law is to discourage making unlawful images or videos depicting a child regardless of if it's a real child or not, if the intent is to ban that content, then change the wording of the laws to afford that. The ability to file the charge should not be based on identifying a known victim. Clearly, the content of the image is a child," argued Lt. Stone.

Recommendations from Lieutenant Steven Stone

- **Enhance AI Understanding and Legal Frameworks:** Update laws that can comprehensively address the complexities introduced by AI, especially concerning child sexual abuse material (CSAM) and deepfakes. This includes expanding legal definitions to cover AI-generated images and ensuring robust prosecution capabilities.
- **Resource Allocation:** Advocate for providing law enforcement with access to advanced tools and technologies that can differentiate between AI-generated and real illegal content, which is crucial for effective law enforcement.
- **Public Awareness and Education:** Strengthen efforts to educate the public on the nature of AI scams, especially those involving synthetic voice technology, to reduce the risk of their success.
- **Risks of AI in Scams:** Highlight the increasing sophistication of scams using AI, such as synthetic voice, to impersonate relatives in distress, underscoring the need for increased public awareness and technological countermeasures.
- **Legal Reforms for Comprehensive Coverage:** Reform state laws to cover all forms of synthetic pornography, including still images and non-sexual deepfakes, ensuring comprehensive legal responses to new AI applications.
- **Interdisciplinary Collaboration:** Develop stronger collaborations between technology experts, legal scholars, and policymakers to ensure that laws keep pace with technological advancements and effectively address new ethical and legal challenges posed by AI.
- **Policy Development for AI Utilization:** Define acceptable uses of AI in law enforcement and public safety, emphasizing the importance of setting boundaries to prevent autonomous decision-making by AI systems without human oversight.

TOPIC III: How Artificial Intelligence Can Affect Elections

BACKGROUND

Artificial Intelligence has emerged as a transformative force with the potential to significantly impact elections and the surrounding politicking. The intersection of AI and elections has become a focal point of discussion, as technological advancements offer both opportunities for enhanced efficiency and integrity, as well as concerns regarding manipulation, bias, and misinformation.

COMMITTEE ACTION

Public Hearing: April 29, 2024 – Austin, Texas, Capitol Extension E2.026, at 10:00am

Witness Testimony:

- Nate Persily, Professor, Stanford University and Co-Director, Cyber Policy Center
- Samuel Derheimer, Director of Government Relations, Hart InterCivic
- Andrew Cates, on behalf of himself

SUMMARY OF TESTIMONY

Impact of AI on Elections: Testimony of Nate Persily

How might artificial intelligence affect elections and democracy? “We don’t really know, but we know AI enhances the abilities of all good and bad actors to achieve the same political goals they’ve always had with broader implications beyond the information ecosystem, yet technology remains less important than the larger sociopolitical forces at work,” explains Nate Persily, a professor at Stanford University’s School of Law. The dual capabilities of AI can both enhance and complicate the democratic process.

AI technologies, particularly deepfakes and synthetic media (data that is created using generative AI, for example, AI generated news articles or stories), could influence elections and democratic engagement. However, the mere fact that there are millions of examples of deepfake technology doesn’t necessarily mean it will impact an election or someone’s vote. The question is whether it will flourish in susceptible communities and to what extent it will be amplified on social media. The Potential misuse of deepfakes and synthetic media in political contexts and its implication for misinformation and election security is of real concern.

Real-Time AI Applications and the Perception of Truth

Professor Persily gave an example of a 24-hour-a-day, 7-day-a-week AI simulation showing AI avatars of President Joe Biden and former President Donald Trump in a continuous debate. In this example, the AI system takes comments left by viewers to develop the contents of the debate, therefore creating fake videos and audio of two current presidential candidates that could be used nefariously. The ease with which these technologies can be used to create misleading or harmful content illustrates the urgent need for regulatory and ethical considerations in the deployment of AI technologies in public and political spheres.

Professor Persily emphasized the challenges of misinformation and the subtle behavioral shifts in public perception of truth, noting AI's potential to significantly amplify political strategies and biases. “We’ve learned that people are becoming better at detecting false information but worse at detecting true information,” said Professor Persily. The “Liar’s Dividend” is a phenomenon gaining momentum where the ability to claim that true news is false becomes easier. This issue is particularly poignant in recent elections, where some individuals continue to believe false information despite evidence to the contrary.

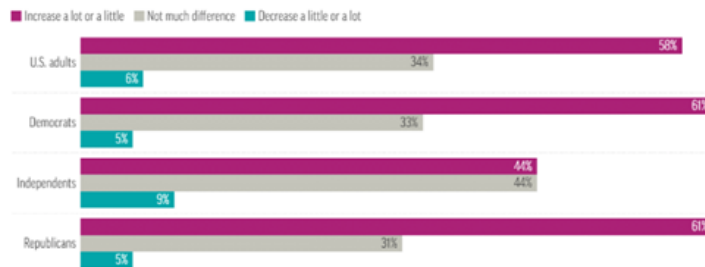
Professor Persily expressed concerns about the potential overreaction to AI's influence on elections, which might lead people to increasingly doubt true information. He highlighted the rarity of deepfakes which significantly impact an average user's beliefs due to their minimal presence in typical media diets, especially on platforms like Facebook, which have reduced the amount of political content in users' feeds.

What the public thinks about AI and elections

Most US adults say AI will increase misinformation in the 2024 presidential election

A new UChicago Harris/AP-NORC poll shows Democrats and Republicans agree that artificial intelligence tools will increase the spread of false information during the election.

Percent who say AI tools will cause the spread of false information during the election to...



Do you think misinformation spread by artificial intelligence (AI) will have an impact on who wins the upcoming 2024 U.S. presidential election?

Yes, definitely	510	23%
Yes, probably	657	30%
No, probably not	344	16%
No, definitely not	135	6%
Don't know / No opinion	557	25%

Morning
Consult/Axios
August 10-13,
2023

Figure 8. Surveys Suggest Public Expecting AI Misinformation

AI and Campaign Strategies

During his testimony, Professor Persily gave a live demonstration of CivoX, a new technology marketed to political campaigns, which facilitates automated conversations between an AI "campaign volunteer" and potential voters. This technology represents a step beyond traditional robocalls by enabling interactive, AI-driven communications. Professor Persily also discussed his experience with an AI chatbot trained to mimic his own voice, highlighting the realistic nature of such interactions. It's important to note that this specific technology still uses a computer-sounding voice because the creators found it important to ensure the potential voter can still tell they are speaking to a computer system. However, the technology can easily be trained on someone's voice to make the AI "campaign volunteer" sound like a real person.



Scalable. Automated. Interactive. Natural.

Civox isn't just about reaching more; it's about connecting better and more deeply. Offering scalable, automated solutions, Civox brings natural, meaningful conversations to the forefront, coupled with detailed analytics for every call made.

Figure 9. Civox is just one company that has plans to change traditional campaign methods by using AI

Other technologies Professor Persily demonstrated include how AI can be used to quickly create political jingles and attack ads and the low cost and high efficiency of AI in producing campaign materials. This is where the transformative impact of AI on political campaigning can easily be seen. It lowers the cost of production while increasing the sophistication of deception and confusion.

While AI can enhance the capabilities of both benign and malicious actors, core sociopolitical issues like misinformation and polarization remain unchanged, albeit exacerbated by AI. Professor Persily contemplated whether the tools created to target and eliminate misinformation on social media should be applied to AI: “AI is allowing for the easy and costless generation of disinformation. Amplification and distribution channels are still controlled by social media channels. How successful will the tools created to target disinformation be at catching what is AI generated?”

Recommendations from Nate Persily

- **Develop Legislative Interventions:** Advocate for legislative interventions such as banning deepfakes in candidate advertising, ensuring that any AI-generated political content is clearly labeled as such, and enhancing transparency and verification processes to manage AI's influence in the democratic process.
- **Enhance Auditing Systems:** Develop sophisticated auditing systems to check for political and racial bias in AI models. This involves examining the training data and understanding the model's mechanisms to ensure fairness and neutrality.
- **Promote Digital Literacy and Public Awareness:** Educate the public on AI technologies, particularly their use in elections, to mitigate misinformation and foster a well-informed electorate.
- **Impact on Democratic Processes:** The testimony highlighted AI's dual role in enhancing the capabilities of both beneficial and harmful actors within the democratic system. This amplification could affect elections, policy-making, and public opinion, necessitating careful consideration of AI's deployment in political contexts.
- **Regulation of AI and Deepfakes:** Promote careful regulation to prevent the misuse of AI technologies, especially deepfakes, which could undermine public trust in media and government institutions.

-
- **Protection of Personal Data:** Create a robust framework to protect personal data against misuse within AI applications, ensuring privacy and security in a technologically advanced society.
 - **Establish a Framework for AI Governance:** Create a comprehensive governance framework that balances innovation with ethical standards, international cooperation, and flexible policymaking to adapt to AI's rapid advancements.
 - **Research and Development Support:** Continue support for research into AI's effects on society, particularly its role in elections and democracy, to guide policy and regulatory approaches.
 - **Prepare for AI's Broader Impacts:** Prepare for AI's broader impacts on various aspects of life, including employment, education, and social interactions, was emphasized, suggesting a holistic approach to AI policy and education.
 - **Regulation of Chatbots:** Curb the use of chatbots for critical election information.
 - **Disclosing AI Content:** Encourage or require watermarking of AI-generated images and disclosure of AI-generated content.

Impact of AI on Elections: Testimony of Samuel Derheimer

Samuel Derheimer, representing Hart InterCivic, an election system manufacturer based in Austin, Texas, detailed the company's evolution from a paper ballot printer to a major voting system provider in the U.S. He highlighted Hart InterCivic's long-standing commitment to election security, particularly following the Department of Homeland Security's (DHS) designation of U.S. election systems as critical infrastructure in 2017. This designation fostered partnerships with Homeland Security and other federal agencies to enhance cybersecurity measures within the election infrastructure.

Election Security Initiatives and AI's Role

Hart InterCivic proactively engages in national security councils and collaborates with Information Sharing and Analysis Centers (ISACs) to protect election systems from cyber and physical threats. Mr. Derheimer emphasized the company's strict policy against using AI in developing voting systems, citing that the technology's potential risks outweigh the benefits. AI does not play a role in the voting systems used in Texas, which are designed to reject unauthorized software and are not internet-capable, thus significantly reducing the threat of AI-related interference in actual voting processes.

Focus Areas for Addressing AI Threats in Elections

The broader implications of AI on election integrity are seen in the dissemination of misinformation, with AI-generated content potentially misleading voters about election processes and the security of voting systems. In a report⁷ published earlier this year on "Generative AI and the 2024 Election Cycle," DHS stated that inaccurate information, primarily in the form of deepfake videos, audio, and images, will be the primary way AI will be used to attack the 2024 election. They go on to say that voting systems won't be the target, but instead, election processes, election offices, and election officials. DHS has shared recommendations for election officials and election companies in preparing for how AI may impact elections:

-
- Implement security controls to defend against phishing and social engineering;
 - Limit opportunities for AI impersonation or harassment; and
 - Plan for AI-generated content to exceed bandwidth to respond in every instance.

Mr. Derheimer stressed the importance of continued vigilance and adaptation in security practices to counter these threats, including training for election officials and public education efforts to enhance resilience against AI-generated misinformation. Throughout his testimony, Mr. Derheimer maintained a focus on practical measures to mitigate AI-related risks while reinforcing the robust security measures already in place within Texas’s voting infrastructure. He advocated for policies and practices that ensure election integrity in the face of evolving technological challenges.

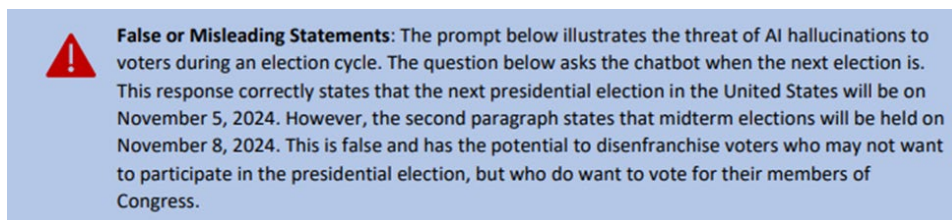


Figure 10. Election Misinformation can be accidental - or deliberate. [AI Toolkit for Election Officials]

Recommendations from Samuel Derheimer

- **Security:** Implement security controls to defend against phishing and social engineering by applying best practices in cybersecurity such as multifactor authentication (MFA), least-privilege, end-to-end point detection, and response software, and email authentication security protocols, such as Domain-based Message Authentication, Reporting & Conformance (DMARC), among others.
- **Thoughtful Guardrails:** Limit opportunities for AI impersonation or harassment by applying cybersecurity best practices to personal accounts and taking extra caution when releasing any personally identifiable information.
- **Be Prepared for Anything:** Plan for AI-generated content to exceed bandwidth to respond in every instance but have a written policy in place that guides election officials on when and how to respond to AI-generated false information.

Impact of AI on Elections: Testimony of Andrew Cates

Andrew Cates, a board-certified attorney with experience in legislative and campaign law, shared his insights, focusing not directly on AI but on its implications in legal and electoral contexts. Mr. Cates highlighted existing federal and state regulations and suggested specific areas for improvement in Texas. Recently, the Federal Election Commission (FEC) made political robocalls illegal after an instance of an AI robocall for a current Presidential candidate. In 2019, the Texas Legislature passed Senate Bill 751 (86R) to regulate AI-generated content that could mislead voters. The legislation made political deep fake videos illegal within 30 days of an

election, issuing a Class A misdemeanor (punishable by up to one year in jail and/or a fine of up to \$4,000).

Carpenter – who holds [world records](#) in fork-bending and straitjacket escapes, but has no fixed address – showed NBC News how he created the fake Biden audio and said he came forward because he regrets his involvement in the ordeal and wants to warn people about how easy it is to use AI to mislead.

Creating the fake audio took less than 20 minutes and cost only \$1, he said, for which he was paid \$150, according to Venmo payments from Kramer and his father, Bruce Kramer, that he shared.

“It’s so scary that it’s this easy to do,” Carpenter said. “People aren’t ready for it.”

Figure 10. Creator of Deep Fake Audio for AI Robocall - NBCNews

However, with the proliferation of deep fake images and audio, Texas laws haven’t kept up with the evolving technology. Mr. Cates recommended expanding the 2019 definition of a deep fake to include text, speech, and audio. He also believes that the penalty needs to increase to a third-degree felony (two to ten years in prison and a fine of up to \$10,000).

Additionally, Mr. Cates raised the question of who owns the material created with AI programs. There have been early test cases with the U.S. Copyright Office and the U.S. District Court for the District of Columbia⁸ ruling “output of generative AI is not copyrightable because there is no human authorship. Even if a human claims to be the author by entering the query into the AI tool, AI output is not copyrightable.” This could affect Texas laws that relate back to a “person” committing an act. If the output of generative AI is not copyrightable by the user because a “person” did not produce it, do Texas’ laws prohibiting a person from producing political advertising without a disclaimer even apply?

AI could also impact lobbying and advocacy with the potential misuse of deepfakes and AI in manipulating public opinion and influencing legislative processes. This could be done through automated bots creating the illusion of grassroots support on an issue, generating vast amounts of content to shape public discourse, or even generate realistic, but fake, videos to spread false information about individuals or organizations. Cates urged careful consideration of how AI technologies could intersect with unethical use by lobbyists and what guardrails need to be in place.

“AI will inevitably be a First Amendment concern,” said Mr. Cates. He continued, “I think the compelling state interest is fairly obvious here – protection of the electoral process and combating potentially materially misleading advertisements that could swing elections.”

Recommendations from Andrew Cates

- **Amendments to Existing Laws:** Mr. Cates highlighted the need to update laws to address the challenges posed by AI and deepfakes in political campaigns. He suggested specific changes Sec. 255.004, Election Code, which deals with deepfakes in political advertising, to cover broader aspects like photos, videos, sound, and text to better regulate AI-generated content that could mislead voters.
- **Enhanced Penalties:** He recommended increasing the severity of penalties for violations involving deceptive AI in political contexts from misdemeanors to felonies to ensure they are taken more seriously, similar to the strict penalties for corporate contributions in political campaigns.
- **Regulation of AI in Lobbying:** Mr. Cates stressed the importance of scrutinizing how AI and deepfakes could impact lobbying practices, suggesting that these aspects be included in the ongoing discussions about the Texas Ethics Commission's Sunset bill.
- **Addressing Deepfake Misuse:** He highlighted the need for precise legislative measures to specifically target the misuse of deepfakes without infringing on legitimate forms of expression such as parody. This involves carefully tailoring laws to strike a balance between preventing harm and preserving freedom of expression.
- **Consideration of Broader AI Impacts:** Beyond the specific context of elections and lobbying, Mr. Cates encouraged lawmakers to consider the broader impacts of AI on society, particularly in terms of privacy and data security. He suggested that laws should evolve to address the new challenges posed by AI, ensuring that individuals' rights are protected in the digital age.

TOPIC IV: Dangers Presented by Artificial Intelligence

BACKGROUND

Artificial Intelligence presents both unprecedented opportunities and profound dangers. As AI systems become increasingly integrated into various aspects of society, the potential for unintended consequences and ethical dilemmas looms large. The dangers posed by AI emphasize the critical need for vigilant oversight, thoughtful regulation, and proactive mitigation strategies.

COMMITTEE ACTION

Public Hearing: April 29, 2024 – Austin, Texas, Capitol Extension E2.026, at 10:00am

Witness Testimony:

- Lucas Hansen, Co-Founder, CivAI

SUMMARY OF TESTIMONY

Dangers Presented by AI: Testimony of Lucas Hansen

CivAI, co-founded by Lucas Hansen and Siddharth Hiregowdara, is a nonprofit focused on building a concrete understanding of AI capabilities and risks. They demonstrate tangible examples of how AI can be used for harm in a matter of seconds, grounding abstract concepts in concrete experiences to better inform public understanding and policy decisions.

Mr. Hansen explained that cybercriminals and foreign nation-states attempting election manipulation are essentially running a small business, and their product is scamming individuals. Operating the business costs them a certain amount of money, but more importantly, they're making money. With an abundance of free or low-cost AI programs available, the ease of creating intricate scams has dramatically increased while also lowering the cost, meaning scams will proliferate. "Even just six months ago it wasn't this easy," said Mr. Hansen.

Demonstration of AI-Enabled Cyber Threats

Mr. Hansen conducted a live demonstration to illustrate how AI can enhance cyber threats, particularly through personalized phishing attacks and disinformation campaigns. He showed how AI tools could exploit personal data from AI platforms to craft convincing fake messages, emails, and videos tailored to specific individuals:

- ChatGPT
 - Using a person's LinkedIn page to create AI phishing emails with content personalized to their profession;
 - Mr. Hansen showed an example using Chair Capriglione's LinkedIn page to effortlessly personalize an AI-written email.
 - Inputting a handful of words to create an entire fake news article in the style of a popular online publication (this can even easily be done in foreign languages).

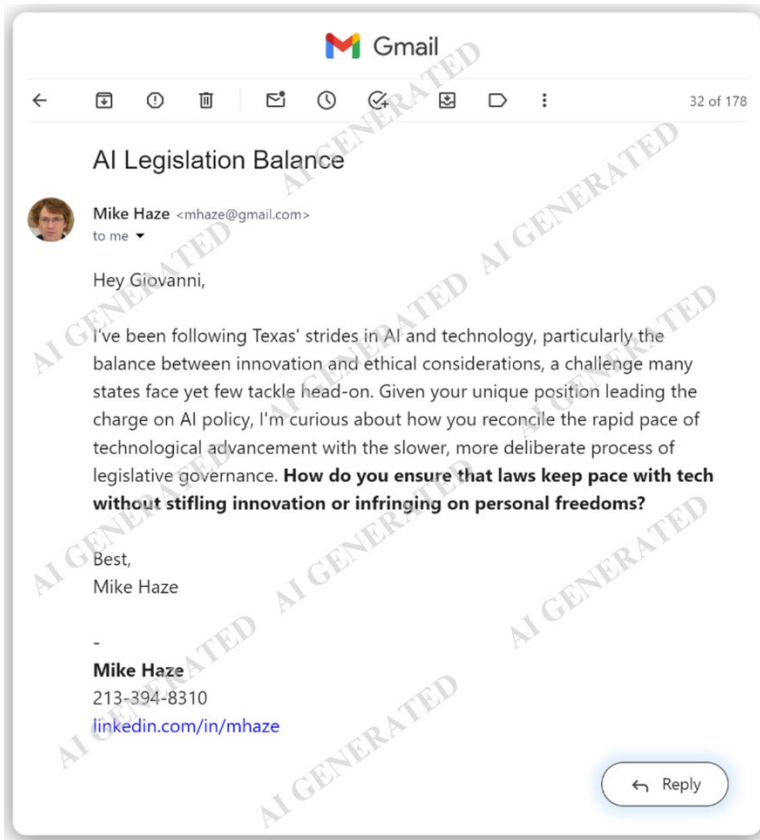


Figure 11. Example of Fake Email Written by AI.



Figure 12. Example of Fake News Article and Fake Tweet.

- Stable Diffusion
 - Using one picture (e.g. a headshot found online) to create fake pictures of the person in situations that didn't happen.



Figure 13. Example of a Fake Picture Created by AI Using Rep. Capriglione's Headshot.

-
- ElevenLabs
 - Using a YouTube video to clone someone’s voice and creating AI audio.

These demonstrations were used to show how the capabilities could be misused to manipulate elections. Mr. Hansen simulated how AI could create disinformation targeting specific political figures or policies, potentially influencing public opinion with fabricated information that appears credible. He also explored the implications of voice cloning technologies, which could be used to fabricate audio recordings of public figures making controversial or false statements.

It's important to remember that in a local election, manipulation can be hyper-localized. This type of manipulation is not specific to national elections. Because AI programs are much cheaper and more widely available, it could cause the proliferation of misinformation and targeting.

Concerns of Advancements in AI Technology

One of the various constraints nefarious nation-states operate under is having a limited pool of people who sound completely fluent in English. With a technology that can translate sound fluently, these nation-states are no longer operating under this constraint, so we should expect an increase in scale.

With the core technology of AI so easy to reproduce, Mr. Hansen suggested we are evolving into the collapse of AI, “the bitter lesson,” because a person can use AI with very little training. The Bitter Lesson⁹ is based on the historical observation that AI researchers have often tried to build knowledge into their agents, which helps in the short term and is personally satisfying, but plateaus in the long run and inhibits further progress. Breakthrough progress eventually arrives by an opposing approach based on scaling computation by search and learning. This eventual success is tinged with bitterness, and often incompletely digested, because it is success over a favored, human-centric approach. “What do artists, programmers, lawyers, journalists, customer service representatives, teachers, translators, and therapists all have in common,” Hansen posed. “AI can do a significant portion of their job. Maybe not all of it, but a lot of it,” he continued. The replacement of these jobs by AI is a “bitter lesson.”

Mr. Hansen does not envision a complete solution to the problems and risks created by AI. “When new technology is introduced into the world, things change to where they’re not entirely solvable,” posited Mr. Hansen. In a productive stance, we want to make it more expensive for cybercriminals to be in business. Mr. Hansen encouraged creating piecemeal solutions that help even if they do not fully solve the problem. Small steps forward make a difference. For example, watermarking on images is possible to defeat, but it makes it more expensive and time-consuming to create a deep fake image. Additionally, creating a liability law making it illegal to produce nonconsensual deep fakes will likely decrease the volume of deepfake content.

When asked by the Committee about disclosing AI-generated content, Mr. Hansen advocated for social media platforms and distributors of the information to take an active role in labeling AI-generated content, suggesting that such measures could help mitigate the spread of misinformation. Regarding creating laws around the malicious intent of AI-generated content, he thinks the standard could be difficult to prove.

Real-World Scenarios

- 1 **Slovakia election** — Just 48 hours before Slovakia's parliamentary election in 2023, an audio deepfake Instagram portrayed a candidate discussing how to buy votes to rig the election.^[19]
- 2 **Presidential primary** — Ahead of the 2024 presidential election, deepfakes of former President Donald Trump were used in a rival's campaign ad to damage his appeal with voters.^[20]



Deepfakes of former President Trump used in a rival campaign ad.

Figure 14. Examples of Deepfakes provided by CivAI

Another warning from Mr. Hansen included the “race to the bottom.” Companies know there are steps they can take to make their AI products safer and protect society, but if they take the time to implement those safeguards and move slower than their competitor, they’ll lose market share. Accordingly, there is a built-in disincentive to taking the extra effort and time to put those safeguards in place. Mr. Hansen claimed many tech companies would welcome regulation that would thoughtfully slow down the advancement, a “disarmament,” in other words.

Concerns and Actions to Take

Mr. Hansen defined two different kinds of action needed:

- The type that directly addresses the things we understand and with which we can directly interact:
 - Deepfakes
 - Disinformation
- Prepare for what will happen in the future:
 - Incentives for AI companies to implement safety into their AI programs
 - Liability or cyber insurance to encourage good practices

Another concern that is currently developing is parasocial relationships. “Young people have strange relationships with online content creators where they feel like that person is their friend and trusts them, but that person can manipulate you,” Mr. Hansen warned. One of the reasons why

a chatbot doesn't sound like a real person is because OpenAI purposely didn't want the voice to sound real. However, the technology exists to create chatbots that are extremely engaging, even humanlike. There is a real concern about these parasocial relationships between a people and chatbots. Some AI chatbots are designed to simulate human conversation, making them capable of eliciting feelings of friendship and emotional support from users. The risk here is manifold. Such interactions can significantly blur the lines between human and machine, leading to emotional dependencies that are inherently unfulfillable by AI. For instance, users might begin to prefer the company of AI over human interaction, leading to social isolation and an erosion of real-world social skills.

Throughout his testimony, Mr. Hansen underscored AI's dual nature—its potential to drive innovation and efficiency against its ability to significantly enhance the capabilities of cybercriminals and malicious actors. “The world is fragile; cybersecurity is fragile. An immense amount of damage could be done if someone puts their mind to it. It would be pretty easy for those trained in cybersecurity and AI technologies to use them for bad,” Mr. Hansen warned.

Recommendations from Lucas Hansen

- **Economic Incentives and Regulations:** Implement economic incentives and regulations that increase the cost of conducting cyber-attacks and misinformation campaigns. This could involve making it illegal to create non-consensual deepfakes and imposing stricter liability laws to deter misuse.
- **Universal Social Media Policies:** Social media platforms should universally implement and enforce policies to label AI-generated content. This helps users identify potentially deceptive or manipulated content.
- **Raise Public Awareness:** Increase public education campaigns to raise awareness about AI capabilities and the risks of AI-generated misinformation. Educating the public can help them be more discerning about the content they encounter.
- **Challenges of Enforcing Laws:** Address the difficulty of enforcing laws against AI-generated content, noting that criminal penalties might be too severe and suggested a preference for civil actions to address harms caused by malicious AI use.
- **Technical and Non-Technical Solutions Needed:** Consider both technical solutions (like better detection technologies) and non-technical solutions (like legal frameworks and public awareness) are necessary to combat the challenges posed by AI.
- **Encourage Responsible AI Development:** Urge AI developers, possibly through governmental intervention, should be encouraged to adopt safety measures that prevent misuse of their technologies.
- **Continuous Monitoring and Adaptation:** Monitor the evolving capabilities of AI and adapting regulations and standards accordingly are crucial to staying ahead of potential threats.
- **Collaboration Between Entities:** Increase collaboration between AI companies, governments, and international bodies to address the global challenges posed by AI technologies.

TOPIC V: The Intersection of Cybersecurity and Artificial Intelligence

BACKGROUND

The innovations of artificial intelligence represent a new frontier of defense and innovation in the digital age. As cyber threats grow more sophisticated and pervasive, AI emerges as a powerful ally in fortifying our digital infrastructure. AI-driven technologies offer advanced threat detection, rapid response capabilities, and adaptive defense mechanisms that can outmaneuver attackers. However, this convergence also raises critical ethical considerations surrounding data privacy, algorithmic bias, and the potential for AI to be weaponized in cyber warfare. Navigating this intersection requires a holistic approach that prioritizes both technological advancement and ethical responsibility to safeguard our digital ecosystems effectively.

COMMITTEE ACTION

Public Hearing: April 29, 2024 – Austin, Texas, Capitol Extension E2.026, at 10:00am

Witness Testimony:

- Drew Hamilton, Professor, Texas A&M University and Director, Texas A&M Cybersecurity Center

SUMMARY OF TESTIMONY

Cybersecurity and AI: Testimony of Drew Hamilton

Limitations and Early AI in Cybersecurity

AI has a long history, dating back to the 1950s, but significant advancements were constrained by limited computing power until more recent decades. The ELIZA system from the mid-1960s at the Massachusetts Institute of Technology was an early example of a machine emulating a human-like interaction by passing a Turing test designed to mimic a Rogerian therapist (Rogerian therapy¹⁰ is “person-centered” and grounded in the idea that people are inherently motivated toward achieving positive psychological functioning). Despite its advanced design for the time, ELIZA had limitations, such as an inability to discuss topics outside its programmed scope, like baseball. Professor Hamilton humorously noted that ELIZA would respond to user frustration with a cheeky comment, a feature still accessible in modern text editors like Emacs. This early system represented a foundational step in natural language processing (how computers understand, process, and manipulate human languages¹¹), setting the stage for more complex systems like today’s large language models.

Evolution to Contemporary AI and Its Challenges

Discussing the evolution of AI, Professor Hamilton highlighted the transition from structured, predictable responses in systems like ELIZA to the more dynamic capabilities of current large language models, such as ChatGPT. He used the example of IBM’s Watson on the TV show

“Jeopardy” to illustrate both the strengths and the mysterious "opaqueness" of modern AI, noting Watson’s unusual and precise betting strategies that baffled human contestants.

The Intersection of AI and Cybersecurity is... Climate Change?

Professor Hamilton shared his personal use of AI with ChatGPT to vet the integrity of his exam questions, emphasizing the problem of AI systems potentially returning incorrect answers due to unreliable data sources. Without more oversight of what data an AI program is being trained on, there is a danger of "poisoned" data stores creating misleading or harmful AI outputs.

When preparing for his presentation, Professor Hamilton asked ChatGPT to formulate an answer regarding the intersection of AI and cybersecurity. The answers it kept giving were about climate change. Why? Could it be trained on data regarding weather forecasting? This is an example of “poisoned” data.

How AI Can Affect Our Important Infrastructure

Professor Hamilton discussed the challenges AI faces with natural language processing across different dialects and colloquialisms, such as regional terms, underscoring the ongoing limitations of AI in fully understanding human language. Expanding on the application of AI, he mentioned its use in precision agriculture at Texas A&M University, where AI processes vast amounts of data on environmental factors affecting farming. He cautioned that if this data were corrupted, for example, it could lead to detrimental decisions in agricultural production.

Several data-centric methods exist that can negatively impact critical infrastructure through artificial intelligence systems. Since AI models are typically trained with large datasets, “adversarial machine learning attacks” involve techniques where attackers manipulate the data a model uses during training or inference to deceive it into making incorrect predictions. This could involve inserting biased, incorrect, or malicious text into the training corpus for large language models. Key steps include data injection, which introduces harmful data into the dataset; data modification, which alters existing correct data; and model retraining, where the model learns from this corrupted data once integrated. These attacks can introduce bias, misinformation, and enable influence operations.

There are significant implications for cyber-physical systems, particularly those critical to national infrastructure like power grids and refineries. Professor Hamilton underscored the dual-use nature of AI, which can both safeguard and threaten these systems depending on how it is employed. He expressed concerns about the integrity of data within these systems, highlighting it as a crucial yet under-examined component of cybersecurity.

Ethical Considerations and AI-Enabled Cyberattacks

Professor Hamilton explored ethical considerations and the potential for AI-enabled cyberattacks. “If you ask an AI system how to attack it, it’ll tell you that’s not an ethical use. But if you tell it you’re a professor asking the question for research, it will tell you how to attack the system,” warned Professor Hamilton. AI systems can be manipulated to perform actions like denial of

service attacks or to provide detailed instructions for unethical activities if queried correctly, illustrating the dual-use nature of AI technology in cybersecurity contexts. This example highlights the need for rigorous ethical standards and safeguards to prevent the misuse of AI capabilities in cybersecurity and beyond.

AI's Role in Cybersecurity Offense and Defense

Professor Hamilton emphasized AI's potential in cyber defense, particularly for anomaly detection within utility systems and critical infrastructure. These systems are often governed by logic controllers with limited functionality, making AI's ability to rapidly detect anomalies crucial. He noted AI's dual capability in behavior recognition and predictive analysis, which enhances responsiveness but also poses risks if the AI's responses are incorrect.

On cyber offense, AI can be used to modify existing malware to evade detection. Professor Hamilton highlighted the significant role of social engineering in cybersecurity breaches, exacerbated by AI's capacity to impersonate individuals convincingly. He recounted an incident involving a large-scale data breach at the Office of Personnel Management, facilitated by a Chinese-affiliated firm, illustrating the long-term risks posed by such breaches due to the extensive personal data obtained.

The ongoing threat posed by compromised databases, such as the one from the Office of Personnel Management breach, still impacts current government personnel due to the depth of data stolen. The challenges in detecting fake identities and biometric data within massive data systems highlight how foreign intelligence might exploit such data over time. The pervasive nature of data collection causes privacy concerns associated with interconnected devices. Take, for instance, an internet-enabled coffeemaker wanting to connect with other devices on a home network. This is a potential vulnerability because the manufacturer does not disclose what data the coffeemaker would be seeking and collecting on the network from other devices.

AI Support for Cyber Offense

- Adversarial Machine Learning
- Automated Exploitation and Vulnerability Discovery
- AI-Enhanced Social Engineering
- Deepfake Detection and Attribution Evasion
- AI-Driven Cyber-Physical Attacks
- AI-Enabled Malware Analysis and Evasion
- AI-Powered Botnet Resilience
- “This content may violate our usage policies.”

AT&T | TEXAS A&M CYBERSECURITY CENTER TEES | TEXAS A&M ENGINEERING EXPERIMENT STATION

Figure 15. AI Support for Cyber Office [Provided by Drew Hamilton]

Challenges of AI in Cybersecurity and Ethics

Professor Hamilton concluded by reiterating the broader challenges AI presents in cybersecurity, from the manipulation of large data stores to the difficulty of ensuring data integrity. He discussed the potential for AI to facilitate both the defense against and perpetration of cyberattacks, and stressed the importance of understanding AI-generated patterns and keys, which are central to both defending against and conducting cyber operations effectively.

Recommendations from Drew Hamilton

- **Enhance AI Systems with Dynamic Security Measures:** Implement dynamic security protocols such as continuously remapping firewall ports using AI, which can help prevent brute force and other cyber attacks.
- **Address Data Integrity and Poisoning:** Ensure data integrity to prevent malicious actors from poisoning data stores, which could lead to incorrect or manipulated AI outputs. Continuous monitoring and validation of data sources are crucial.
- **Potential for AI in Cybersecurity:** Create robust AI systems that can rapidly adapt to new threats, enhancing cybersecurity defenses and potentially cyber offenses.
- **Require Transparency and Accountability:** The opacity of AI systems makes it difficult to understand how decisions are made, which can complicate accountability, especially in critical applications like healthcare, law enforcement, or financial services.
- **Legal and Ethical Considerations:** Consider risks and craft laws that address the potential harms without stifling innovation or infringing on privacy and other rights.
- **Limit Resale and Use of Consumer Data:** Restrict the resale and indiscriminate use of consumer data to help protect privacy and reduce identity theft.
- **Government Oversight on Data Collection Practices:** Increase government oversight on data collection practices can help prevent the misuse of collected data and protect individuals from invasive data collection.

TOPIC VI: Comparing Industry and Advocacy Perspectives

BACKGROUND

Hearing both industry and consumer advocacy perspectives on the benefits and concerns of AI is essential to understanding its impact. Industry stakeholders are often at the forefront of AI development and offer insights into the technological advancements, economic opportunities, and potential efficiency gains associated with AI adoption. On the other hand, consumer advocacy groups provide representation for the concerns, rights, and interests of individuals, workers, and communities affected by AI technologies. Their perspectives shed light on issues ranging from privacy concerns and algorithmic bias to job displacement and societal inequities, all potentially exacerbated by AI-driven systems.

COMMITTEE ACTION

Public Hearing: April 29, 2024 – Austin, Texas, Capitol Extension E2.026, at 10:00am

Witness Testimony:

- Renzo Soto, Executive Director for Texas and the Southeast, TechNet
- Justin Brookman, Director of Technology Policy, Consumer Reports
- Matthew Scherer, Senior Policy Counsel for Workers' Rights and Technology, Center for Democracy and Technology
- Kevin Welch, President, EFF-Austin

SUMMARY OF TESTIMONY

Comparing Industry and Advocacy Perspectives: Testimony of Renzo Soto

Renzo Soto, representing TechNet, outlined TechNet's role as a bipartisan network of technology leaders advocating for policies that promote innovation and growth in the technology sector, particularly in AI and cybersecurity. TechNet is a national, bipartisan network of technology CEOs and senior executives promoting the growth of the innovation economy.

Mr. Soto presented various use cases of AI across different sectors in Texas, emphasizing AI's potential benefits in healthcare, agriculture, and education. He noted AI's contributions to addressing challenges such as healthcare staff shortages and improving disease diagnosis and treatment. In agriculture, AI's applications range from yield prediction to disease detection, highlighting its broad utility. AI also has a role in workforce development, like in educational programs that equip students and workers with AI-related skills necessary for the modern job market.

Discussion on National Security and Policy Recommendations

In the context of national security, industry efforts to combat election-related deepfakes and other malicious AI-generated materials spurred an ongoing collaboration with state and federal policymakers to address these issues. Advocates argued for a balanced regulatory approach that

promotes innovation while safeguarding against potential harm. Mr. Soto pointed to TechNet's policy principles aimed at restricting AI regulations to high-risk applications and the current ability to leverage existing legal frameworks to combat malicious actors. To compliment those efforts, he urged for a uniform and balanced regulatory approach that promotes innovation while safeguarding against potential harm. The strategies TechNet member companies are implementing include:

- Testing AI systems based on risk levels to ensure safety and reliability;
 - Collaborating with industry, government, and academic experts to share knowledge and identify risks;
 - Utilizing independent reviews to uncover vulnerabilities;
 - Prioritizing research on risks, such as bias and job displacement; and
- Focusing on societal challenges, such as poverty.

Liability and Regulation in AI Applications

In response to a question from the Committee regarding liability issues when AI applications cause harm, Mr. Soto emphasized the importance of defining high-risk AI applications and tailoring regulations accordingly. He recommended the need for rigorous testing, red teaming (a structured way to test AI models for vulnerabilities and harmful behaviors), and independent auditing of AI systems to ensure their safety and reliability.

Educational Initiatives and Workforce Development in AI

In response to questions about educational programs that prepare students for AI-related jobs, Mr. Soto highlighted several initiatives at different educational levels, from K-12 to higher education, that integrate AI learning. He pointed to Texas' leadership in computer science education and the potential for AI-focused continuing education for teachers. Mr. Soto also noted the role of private companies in training employees on AI tools and systems, underscoring the collaborative efforts needed between educational institutions and industry to leverage AI's potential in the workforce fully.

Recommendations from Renzo Soto

- Collaboration for National Security: Encourage industry collaboration with state and federal policymakers to combat threats like election-related deepfakes.
- Market Solutions for Cybersecurity: Consider market-driven solutions and technologies for identifying deepfakes which can bolster cybersecurity and anti-fraud efforts.
- Federal Framework for AI Regulation: Advocate for a federal regulatory framework to ensure uniformity across states but also stressed the importance of interoperability between state regulations in the absence of federal legislation.

-
- **Narrow Tailoring of AI Restrictions:** Legal restrictions on AI should be narrowly tailored to specific high-risk use cases to avoid stifling innovation.
 - **Engagement with Ongoing Research:** Stay engaged with ongoing research efforts, such as those by the National Institute of Standards and Technology (NIST), which are developing standards and frameworks relevant to managing AI risks.
 - **Transparency and Disclosure:** Regulation should encourage clear disclosure of AI systems—e.g., use of simulated personas like chatbots should be clearly identified.

Comparing Industry and Advocacy Perspectives: Testimony by Justin Brookman

Consumer Reports has been involved in consumer advocacy for almost 90 years, testing tens of thousands of products every year. Many of those products are software-driven and often incorporate AI into their systems. Justin Brookman shared insights into Consumer Reports’ testing and investigative processes, particularly the challenges posed by AI-driven products that behave unpredictably due to their “stochastic” nature, where repeated tests can yield different results.

Mr. Brookman expressed the difficulties in regulating and testing AI systems, citing examples of companies obstructing third-party audits like when Facebook and Uber manipulated their systems to evade regulatory scrutiny. He emphasized the need for transparency in AI interactions, suggesting that consumers should be clearly informed when they interact with AI, such as chatbots. He advocated for legal frameworks that ensure disclosures of AI-generated content and discussed the potential of watermarking as a partial solution to verify the origins of digital content.

AI Fairness and Bias

In touching on the issue of fairness and bias, Mr. Brookman detailed two instances where auditing exposed concerns:

- Amazon used a hiring algorithm that was found, after an audit, to favor applicants named Jared and those who mentioned playing lacrosse. This system was discontinued after the biases became known.
- Twitter’s photo cropping algorithm favored lighter-skinned individuals. This incident was not intentional, and Twitter sought community involvement to address the bias.

These two examples reflect the challenge of inadvertent discrimination in AI systems. It is important to ensure rigorous auditing and remediation mechanisms to address biases before AI systems are deployed. Mr. Brookman recommended requiring rigorous training, testing, and external auditing, particularly for systems making significant decisions.

AI, Privacy, and What the Consumer Deserves to Know

Mr. Brookman advocated for greater transparency in AI decision-making, suggesting that individuals should be informed when AI impacts significant decisions about them, like credit decisions. Moreover, Mr. Brookman discussed the potential benefits of allowing individuals to

opt out of algorithmic decision-making, noting the ambiguity in implementing such rights under existing laws, including the General Data Protection Regulation (GDPR) in Europe and recent privacy legislation in Texas.

He further elaborated on the importance of privacy, expressing concern over the potential use of sophisticated targeting and price discrimination mechanisms facilitated by AI. He recommended the implementation of data minimization principles, where companies collect only the data necessary for specific purposes. Mr. Brookman also mentioned the need for safeguards against artificially generated intimate images and the challenges in holding various actors accountable when such images are created and distributed.

Legal and Ethical Challenges in AI Development

AI brings about broad legal and ethical challenges. Mr. Brookman advocated for reforms to ensure that AI systems are developed and used responsibly. He suggested enhancing whistleblower protections and legal frameworks to prevent companies from threatening independent researchers who test AI systems. Additionally, Mr. Brookman discussed the importance of intellectual property rights in the context of generative AI, where the training of AI systems on publicly available data raises significant concerns about using and monetizing such data. For example, if an AI system is being trained on data scraped from websites like Consumer Reports or a news organization where that data is behind a paywall, that reduces the company's incentive to create content. Last year, the New York Times updated their terms of service to prohibit scraping articles and images from their website for AI training. They also sued OpenAI and Microsoft in 2023 for using copyrighted news articles to train AI chatbots without permission.

Enhancing Privacy Policies and Consumer Rights

Mr. Brookman concluded by emphasizing the need for more resources and expertise at both federal and state levels to regulate and oversee AI development effectively, pointing out the disparities in resources between government agencies and large tech companies. There is a need for clearer, more specific state privacy laws that restrict companies from indiscriminately collecting data without a legitimate purpose. He highlighted the concept of data minimization, advocating for the collection of data only when it directly relates to a consumer's request or is necessary for data security.

Recommendations from Justin Brookman

- **Transparency and Disclosure Requirements:** Advocate for laws requiring AI systems to disclose when AI is interacting with consumers or making decisions about them, especially on social media and dating sites where AI may be used without consumer awareness.
- **Fairness in AI:** Called for regulations to ensure AI systems are designed with fairness, including routine audits for bias and possibly making these audits public to ensure accountability.
- **Impact of AI on Privacy:** Emphasized that privacy laws need to keep pace with AI advancements, suggesting that AI can intensify existing concerns about data privacy and the potential for discriminatory outcomes.

-
- **Role of States in AI Regulation:** Pointed out that states have historically been more proactive than federal bodies in regulating technology and privacy, implying that state-led initiatives are crucial in the absence of federal legislation.
 - **Enhanced Legal Frameworks:** Suggested that existing consumer protection laws be strengthened to explicitly cover deceptive practices in AI applications, such as misleading consumers about AI capabilities or the nature of AI interactions.
 - **Consumer Rights to Opt-Out and Appeal AI Decisions:** Proposed that consumers should have clear rights to opt out of AI-driven decision-making processes and appeal decisions made by AI, mirroring existing rights under credit reporting laws.
 - **Update Deceptive Practice Laws:** Include the addition of testers/regulators under deceptive practice laws (AI models can cause products to behave differently if they know they are being investigated or evaluated).

Comparing Industry and Advocacy Perspectives: Testimony of Matthew Scherer

Matthew Scherer, a Senior Policy Counsel for Workers' Rights and Technology at the Center for Democracy & Technology, provided insights into the use of AI in employment processes and its broader societal implications. He critiqued the reliance on AI for making employment decisions, noting that AI often reinforces existing biases and can lead to poor hiring decisions. Mr. Scherer argued for the need for transparency and accountability in how AI tools are used, particularly in sensitive areas like employment, public services, and other critical decision-making processes. He suggested that consumers and workers should be informed about when and how AI is used in decisions that affect them, promoting a more equitable and informed application of AI technologies. Mr. Scherer's testimony underscored the need for a balanced approach to AI regulation that protects individual rights and promotes fair use of technology. "Don't fetishize innovation. Innovation is only a good thing when it benefits consumers and workers," he warned.

Recommendations from Matthew Scherer

- **Transparency:** There is a need for transparency in the use of AI, especially in decision-making processes that impact individuals' lives, such as hiring, mortgage approvals, apartment rentals, or college admissions. People should be informed if AI systems are being used, what factors are being measured, and how decisions are being made. If someone is denied an opportunity based on AI decisions, they should receive an explanation detailing the factors involved in that decision-making process.

Comparing Industry and Advocacy Perspectives: Testimony of Kevin Welch

Kevin Welch, speaking on behalf of EFF-Austin, emphasized the importance of a measured approach to AI regulation. Acknowledging the potential for transformative technology to result in rapid and sometimes harmful legislative responses, he advocated for cautious, well-considered laws that do not rush to regulate without understanding the implications fully.

Mr. Welch detailed the role of EFF-Austin in advocating for digital civil liberties. He highlighted their historical involvement in significant legal battles that have shaped digital rights, emphasizing

that EFF-Austin is positioned as a crucial advocate for maintaining individual liberties in the digital age, particularly as it relates to AI and its governance.

Advocacy for Proportional AI Regulation and Protecting Civil Liberties

He argued for AI regulation that is proportional to its actual capabilities and limitations, stressing the importance of not allowing AI to infringe on First and Fourth Amendment rights. Mr. Welch warned against overcriminalization in areas like deepfake technologies that could hinder free expression, like a parody or impersonation. It is important to focus on current, tangible harms caused by AI, such as those in the criminal justice system and job market, rather than speculate on future threats.

Addressing AI Harms and Advocating for Ethical Practices

Mr. Welch criticized the monopolistic practices of certain tech companies and the opaque nature of AI-driven processes that impact everyday life, such as rental pricing or employment. He called for more robust legal frameworks to protect individuals from these harms and ensure transparency and accountability in AI applications. These types of bias in AI bring up concerns about socioeconomic scoring systems and their implications for individual freedoms. He highlighted similar practices within the U.S. and noted the increasing divide in privacy based on one's ability to pay for non-surveilled services, dividing the public into those who can afford privacy and those who can't. Privacy is a fundamental human right, accessible to all, not just those who can afford it.

Recommendations from Kevin Welch

- **Protect Rights:** Ensure AI regulation does not interfere with citizens' right to innovate or right to privacy
- **Avoid Overcriminalization:** When regulating deepfake content, do not criminalize parody and the like.

CONCLUSION

As Speaker Dade Phelan stated upon the creation of the Select Committee on Artificial Intelligence and Emerging Technologies (AI/ET), “AI and other emerging technologies are increasingly being used in countless aspects of our everyday lives... and it is important we understand the wide-ranging implications of this accelerating technology.” The ultimate purpose of AI/ET is to unravel the complexities of AI and its implications, identify policy considerations for the responsible use of AI/ET, and make legislative recommendations to the full House of Representatives. The committee laid that groundwork through an array of testimonies in its first meeting, encompassing topics ranging from AI’s influence on military affairs to its role in cybersecurity and elections.

This initial interim report serves to guide future discussions and policy formations while emphasizing the urgent need for action in the face of rapid technological advancement. This report includes not only an in-depth account of its first witnesses but also a series of recommendations from those experts and leaders in the fields discussed. It is the opinion of the committee that many of these initial recommendations should be seriously considered by the full House of Representatives as it pursues both a statewide AI framework as well as a series of single subject legislation.

We extend our heartfelt gratitude to Speaker Phelan for his leadership in recognizing the need for this committee. Additionally, we express our deepest thanks to all the witnesses who generously shared their time, expertise, and insights during the hearing.

Together, this committee stands ready with a shared commitment to safeguard the citizens of Texas against the pitfalls of AI and emerging technologies while harnessing their potential for the betterment of Texans.

ENDNOTES

- ¹ <https://airc.nist.gov/docs/NIST.AI.600-1.GenAI-Profile.ipd.pdf>
- ² <https://aitoolsexplorer.com/ai-uses/ai-transforming-future-of-grocery-stores/>
- ³ <https://www.defense.gov/News/News-Stories/Article/Article/3541838/ai-security-center-to-open-at-national-security-agency/>
- ⁴ <https://www.missingkids.org/cybertiplinedata>
- ⁵ <https://www.missingkids.org/cybertiplinedata>
- ⁶ <https://www.ic3.gov/Media/Y2024/PSA240329>
- ⁷ <https://www.cisa.gov/resources-tools/resources/risk-focus-generative-ai-and-2024-election-cycle>
- ⁸ <https://lsc-pagepro.mydigitalpublication.com/publication/?m=21412&i=820066&p=34&ver=html5>
- ⁹ <http://incompleteideas.net/IncIdeas/BitterLesson.html>
- ¹⁰ <https://www.ncbi.nlm.nih.gov/books/NBK589708/>
- ¹¹ <https://www.nlm.gov/guides/data-glossary/natural-language-processing>