ALASKA STATE LEGISLATURE
SENATE STATE AFFAIRS STANDING COMMITTEE
February 6, 2025
3:31 p.m.

MEMBERS PRESENT

Senator Scott Kawasaki, Chair
Senator Jesse Bjorkman, Vice Chair
Senator Elvi Gray-Jackson
Senator Robert Yundt

MEMBERS ABSENT

Senator Bill Wielechowski

COMMITTEE CALENDAR

PRESENTATION(S): AI AND STATE FUNCTIONS

- HEARD

PRESENTATION(S): A.I. DEEPFAKES AND CHATBOTS

- HEARD

PREVIOUS COMMITTEE ACTION

No previous action to record

WITNESS REGISTER

BILL SMITH, Chief Information Officer (CIO)
Office of Information Technology (OIT)
Department of Administration
Anchorage, Alaska
POSITION STATEMENT: Provided the presentation: AI and State Functions.

ILLANA BELLER, Organizing Manager
Public Citizen
Washington D.C.
POSITION STATEMENT: Provided the presentation: A.I. Deepfakes and Chatbots.

ACTION NARRATIVE

3:31:22 PM
CHAIR KAWASAKI called the Senate State Affairs Standing Committee meeting to order at 3:31 p.m. Present at the call to order were Senators Gray-Jackson, Yundt and Chair Kawasaki. Senator Bjorkman arrived thereafter.

PRESENTATION(S): AI and STATE FUNCTIONS

3:32:47 PM
CHAIR KAWASAKI announced the presentation: AI and STATE FUNCTIONS.

3:32:59 PM
BILL SMITH, Chief Information Officer (CIO), Office of Information Technology (OIT), Department of Administration, Anchorage, Alaska, provided the presentation AI and State Functions. He moved to slide 2, Generative Artificial Intelligence (AI) and he defined generative artificial intelligence as; creating systems that can create things that didn't exist before. He stated that the last several years technology has gotten to a point where it can create new things that have not existed before, and technology is able to look at multimodal forms of information. An example would be an image, AI can look at the image and reference other content it has received before; from other places and make assumptions from the information.

3:34:49 PM
MR. SMITH continued slide 2. He stated over the past year or two, state agencies, within the executive branch, have been exploring how AI can meaningfully improve operations. He stated that the focus has been on identifying real use cases—starting with a specific problem and then finding the right tool to address it. The Office of Information Technology (OIT) has led efforts to educate teams on what AI can and cannot do, promote responsible use, and help departments align the right tools with their specific needs. He said OIT has been reviewing data systems to ensure information is secure and AI-ready, while developing clear guidance around the use and security of these tools. He stated that OIT is assessing the existing enterprise tools to see how new AI capabilities can be integrated, so OIT can make the most of what they already have.

3:36:55 PM
CHAIR KAWASAKI announced Senator Bjorkman joined the committee.

3:37:03 PM
MR. SMITH moved to slide 3 and talked about the following artificial intelligence tools:

[Original punctuation provided.]

Generative AI Approaches: End User AI, Developer AI, Custom Build AI

End User AI

Off-the-shelf options with AI embedded in currently used tools.

AI embedded into third-party Software Applications by providers to improve functionality.

Developer AI

Custom AI configuration using existing AI tools.

State of Alaska Professional and Cloud Developer tools-AI tools that allow for secure, custom configuration.

Custom Build AI

Custom AI models from scratch.

Large scale implementation and creation/training of foundational model.

MR. SMITH stated that OIT hasn't seen any big custom build request come to them, but they are working with the review board, so OIT is able to make sure they are asking the requester the right questions and things are done in a responsible manner.

3:40:04 PM
CHAIR KAWASAKI mentioned that Mr. Smith referenced types of questions to ask a custom build AI requester. He asked what are some of the caveats OIT watches for when doing custom build AI.

3:40:31 PM
MR. SMITH responded that when OIT evaluates AI platforms, especially custom builds, we focus on a few key items. First, is data secure and safely used. The AI platforms must follow OIT's security and compliance standards—whether for health, criminal

or other areas. Second, OIT looks at responsible use AI principles like privacy, reliability, and safety to ensure the tool fits its intended use. He said the left two columns of the slide, End User AI and Developer AI, provide OIT with an opportunity to move more rapidly and effectively because they are built with data and in data environments that are secure with the right protocol compliance in place.

3:42:04 PM
MR. SMITH moved to slide 4, Enterprise Artificial Intelligence (AI) Tools. He explained what OIT is doing right now in the executive branch with AI tools. He named some examples: First, OIT already uses AI in cybersecurity systems that monitor network traffic and flag unusual behavior for its teams to check out. Second, OIT is about to pilot AI assistants in office software—like Outlook, Word, and Excel. These tools help summarize emails, draft messages, pull action items from meeting transcripts, and more. It's meant to boost productivity without requiring people to learn new tools. He stated that since there's a cost, OIT will start small, testing the value in real work settings. Then OIT will share what works best so leaders can decide if and where it's worth expanding.

3:45:22 PM
SENATOR BJORKMAN stated that legislators often need to compare two documents and analyze the differences. He said he hasn't found a great AI tool for that yet. He asked if Mr. Smith knew of one he could try.

3:45:44 PM
MR. SMITH answered that he doesn't know of any but will talk with his team to see if there's an AI tool that would compare two documents and analyze the differences.

3:46:22 PM
MR. SMITH continued slide 4. He stated that the next category is "professional" users—those between end users and developers. Think of an accountant who needs to work with data but doesn't code. He said OIT is using tools like Co-Pilot Studio to help build assistants for these users. He noted one example: OIT created a chatbot that understands the security policies. Instead of digging through long documents, an employee can ask a question like, "Can I check the weather on my work computer?" and get a clear answer with a policy reference.

3:47:56 PM

CHAIR KAWASAKI commented on the example given and asked if OIT are double checking the answer AI gives to match what a person would find if they read through all the documents.

3:48:17 PM
MR. SMITH responded that OIT looks for the accurate and controlled data. He stated that part of the testing performed by OIT is proof of concept using a chatbot that pulls from state websites. He stated that it worked well but sometimes gave outdated info—like listing someone no longer in a role. That's because it pulled from an old document and OIT had to tweak it to prioritize newer sources. He said the tool needs both clean data and tuning to get accurate answers. OIT tests both thoroughly.

3:49:44 PM
SENATOR BJORKMAN mentioned complaints that using the ALVIN system through the DMV is very slow. He asked if AI could identify and propose solutions to fix the system like ALVIN.

3:50:29 PM
MR. SMITH answered at this time OIT doesn't have an AI tool for that specifically, but it is the type of thing AI is used for, and the state may have it in the future. He stated that AI is good at solving problems but not good at solving mysteries.

3:51:40 PM
MR. SMITH continued with slide 4. He explained the Developer group needs some IT and programming skills but uses tools already in OIT's cloud setup. He said several departments are working with vendors on AI solutions, made possible by the earlier Rapid Cloud Migration Project, which created secure, compliant cloud spaces for each department. He stated that upgrading Office licenses also enabled access to advanced AI features. These tools run in OIT's private cloud, keeping data secure and allowing faster more confident AI adoption to better serve Alaskans.

3:54:15 PM
CHAIR KAWASAKI said regarding testing the system he asked whether OIT tests for specific things like biases within the system and does the state have a written policy.

3:54:43 PM
MR. SMITH answered that OIT doesn't currently have a specific policy on AI bias, mainly because of the kind of AI OIT is using right now. Most of the tools used are pre-trained models brought

into OIT's secure environment, where AI learns from our own data. Since those models are vetted beforehand, the risk of bias is lower than with public-facing AI. He stated that if OIT moves toward building its own large language models, it will need to be more careful about training and testing for bias. For now, OIT's focus has been on educating employees about handling data responsibly, whether they're using AI, email, or other systems. OIT is updating their acceptable use policy to reflect that.

3:57:30 PM
CHAIR KAWASAKI asked Mr. Smith to explain front facing systems that have an automatic chat bot that answers questions.

3:58:08 PM
MR. SMITH responded that natural language chatbots make it easier for people to get info without needing to phrase things perfectly. AI chatbots remember context so you can have a back-and-forth conversation. He stated many state departments had AI chatbot on their wish list to start implementing it. OIT has been testing several natural language chatbots and plan to roll them out across sites and services soon to reduce friction and make access easier. One early version is already live on the DMV site—it's AI-driven and getting better over time.

4:02:32 PM
At ease.

PRESENTATION(S): A.I. DEEPFAKES and CHATBOTS

4:03:02 PM
CHAIR KAWASAKI reconvened the meeting and announced the Presentation: A.I. Deepfakes and Chatbots

4:05:41 PM
ILLANA BELLER, Organizing Manager, Public Citizen, Washington D.C., provided a presentation A.I. Deepfakes and Chatbots.

4:06:55 PM
MS. BELLER moved to slide 3, What is a deepfake and how are they used in an election's context. She stated that a deepfake is content that is fabricated using technology. This can be done through audio, video or an image. She explained it depicts someone doing or saying something they never did or said in real life. She restated the definition of deepfakes but in reference to election candidates.

4:08:29 PM

MS. BELLER moved to slide 4 and continued to emphasize that deepfakes are more prominent now than before. She stated that a deepfake scandal occurred in Slovakia's election in 2024.

4:10:12 PM
MS. BELLER moved to slide 5. She gave another example of how deepfakes are used in elections. She explained that during the New Hampshire primary, residents received deepfake robocalls of President Biden telling the voters not to vote this election.

4:11:00 PM
MS. BELLER moved to slide 6. She gave another example how deepfakes were used during a political campaign in North Carolina involving a Political Action Committee (PAC) and Mark Walker. She explained the process of how the deepfake occurred and how PAC was supporting candidate A and then PAC circulated a deepfake of candidate B (Mark Walker). She continued with saying the video deepfake showed candidate B telling the public he was not qualified for office and predicting candidate A was going to win the election.

4:12:10 PM
MS. BELLER moved to slide 7 and stated that a long-term consequence of deepfakes is people’s distrust of media.

4:12:48 PM
MS. BELLER moved to slide 8 and explained that technology is improving rapidly. She stated deepfakes are improving in quality, quantity and accessibility. She emphasized how quickly a bad deepfake can circulate and can cause an outsized effect.

4:14:39 PM
MS. BELLER moved to slide 9 and spoke about the following:

[Original punctuation provided.]

Legislation Addressing this Issue.

- 21 states have passed legislation to regulate deepfakes.
- 49 States and D.C. have introduced legislation
  -Mostly in this session and last
  -Most that did not pass was because of time.
- 18 States have already introduced this legislation this session.
- Strong bipartisan support, unanimous votes.

4:15:52 PM
MS. BELLER moved to slide 10 and explained the United States map shows where election deepfake bills passed or are in play as of January 2025. She said the dark blue states passed deepfake bills before 2024. She said the lighter blue represent states that passed deepfake bills in 2024. She said the green represents states that have legislation pending. She stated the deepfake bills are passing in republican and democratic states with an almost nearly unanimous support.

4:16:40 PM
MS. BELLER moved to slide 11 and spoke about the following:

[Original punctuation provided.]

Key Elements of Anti-Fraudulent Deepfake Legislation

- Prohibit distribution of unlabeled deepfakes - **Why disclosure not ban?**

She stated there are a couple bills that are a full ban. She recommends people should require a disclosure instead of a complete ban, it's less likely to be challenged by the first amendment.

- Standards for disclosure - must be very clear and prominent
- Covers all people - not just candidates, parties and committees. e.g. influencers
- Usually within a certain number of days of E-day
- Only covers people who knowingly circulate a deepfake
- Establish a right for affected parties to seek injunction to take it down
- Establishes penalties

4:19:44 PM
MS. BELLER moved to slide 12 and spoke about the following:

[Original punctuation provided.]

Protections

- No liability for broadcasters or platforms that make reasonable effort to prevent deepfakes, or that show deepfakes as part of news coverage and describe as deepfakes

- Satire and parody are protected

- Individuals who are unknowingly reposting are not held liable

4:20:59 PM
MS. BELLER moved to slide 13 and spoke about the following:

[Original punctuation provided.]

Lessons Learned

- **Clear** definitions is critical

  -Depicts someone doing or saying something they never did or said

  -Provides a fundamentally different understanding of the persons speech or behavior

  -Intent to undermine candidates' reputation or otherwise deceive voters

  -Satire and parody exemptions

  -Liability must be on the distributor

4:23:54 PM
MS. BELLER moved to slide 14 and 15, Non-Consensual Intimate Deepfakes and What is an intimate deepfake. She said an intimate deepfake is fabricated content of a sexual act or in the nude, in the form of a video or image that's not real. She stated the intimate deepfakes are more common than election deepfakes.

4:25:08 PM
MS. BELLER moved to slide 16 and spoke about the following:

[Original punctuation provided.]

Pervasiveness of this Problem

- Intimate deepfakes make up 98 percent of all deepfakes
- 99 percent of victims are women
- Children (girls) are a significant percentage of the victims
- A study recently found that 57 percent of those under 18 years of age are concerned about becoming victims to intimate deepfakes and 10 percent of individuals reported being a victim of intimate deepfakes, knowing a victim, or both.
- WIRED found on Telegram at least 50 bots that claim to create explicit photos or videos of people with only a couple of clicks - these bots have over 4 million monthly users

4:26:45 PM
MS. BELLER moved to slide 17, Examples. She mentioned the examples of intimate deepfakes around the world reported by the news.

4:28:15 PM
MS. BELLER moved to slide 18. She read the different types of harm that can be the outcome of being a victim of intimate deepfakes. She said deepfake pornography is being used for sexual extortion, as a result there have been a few cases of suicide.

4:29:41 PM
MS. BELLER moved to slide 19, State Tracker. She discussed the United States map that showed the 30 dark green states that have passed legislation, the light green states have legislation that's pending, the bright green states have passed legislation, but it only covers minors. 4 out of 5 states that passed the child only deepfake laws last year; have now introduced laws that would cover everyone.

4:30:54 PM
MS. BELLER moved to slide 20 and spoke about the following:

[Original punctuation provided.]

Legislation Passed in the States

- 30 states have enacted legislation + 1 more just passed
- 45 states have introduced legislation
- Broad bipartisan support

4:31:20 PM
MS. BELLER moved to slide 21, Model Legislation. She stated that Public Citizen has shared a model bill and have seen states take a few main approaches: about half passed standalone laws, others updated private image or revenge porn laws, and some amended child porn laws when minors are involved. She said for states updating private image laws, it's critical to include "intent" in the criminal section. She stated that's because courts may argue that privacy violations don't apply if the image isn't technically "real," even if it looks just like the person. She emphasized just adding "deepfake" to the definition isn't enough. Intent to harass, threaten, or alarm usually needs to be clearly included. She then spoke about the following:

[Original punctuation provided.]

Model Legislation.

A few important recommendations to keep in mind when drafting this legislation:

1.Provide for both civil liability and criminal penalties. Civil liability can afford the victim injunctive and economic relief while the criminal penalty can act as a deterrent.

2. Allow for a defense of consent but require more than mere assertions of oral consent to satisfy it.

3. Disclaimers of inauthenticity or unauthorized creation should not be permitted as a defense against intimate deepfakes, as such disclosure does not mitigate the reputation and psychological harm done to the victims.

https://www.citizen.org/article/public-citizen-model-state-law-regulating-non-consensual-intimate-deepfakes/

4:34:58 PM

MS. BELLER moved to slide 23. Consumer Protection + Chatbot Labeling. She stated that more people are catching on to chatbots, and some states are starting to require clear disclosure when someone is interacting with one. This applies to both sales bots and bots used in areas like healthcare or legal services. She said the concern is that bots can access personal data and use algorithms to manipulate behavior—like fast food bots upselling based on past orders and people could think they're talking to a doctor or lawyer when it's a bot. She opined it's a simple fix—just make sure users know they're dealing with AI. A few states have passed or introduced laws on this, and it has bipartisan support.

4:38:05 PM
CHAIR KAWASAKI asked how to tell the difference between harmless altered deepfakes and deepfakes that cross a legal and ethical line.

4:38:45 PM
MS. BELLER answered that Public Citizen's model defines synthetic media as manipulated images, audio, or video showing someone's appearance, speech, or conduct. When it comes to deceptive and fraudulent deepfakes are what Public Citizen is seeking to regulate. This type of deepfake is synthetic media that depicts a candidate with the intent to injure their reputation or deceive the voter or mislead voters. She stated that the deepfake must appear real to a reasonable person and show someone saying or doing something they didn't. The key is intent and whether it gives a viewer a fundamentally false impression of what happened. She said minor edits, like removing a mole or adjusting height, wouldn't meet that threshold.

4:41:31 PM
CHAIR KAWASAKI asked if child pornography should be illegal regardless how its presented, by artificial intelligence or not.

4:42:12 PM
MS. BELLER responded that many states are updating existing child pornography laws to include synthetic media and deepfakes. Most of these updates expand the definition to cover not just distribution but also possession—though not all states include possession. She stated that it's up to legislators, but the trend is to tweak current laws to fully cover this content.

4:44:54 PM

There being no further business to come before the committee, Chair Kawasaki adjourned the Senate State Affairs Standing Committee meeting at 4:44 p.m.