Senate Finance

03/11/2025 02:00 PM

SB25-011 Detection Components for Wildfire Mitigation

Typed Text of Testimony Submitted

Name, Position, Representing	Typed Text of Testimony
Mike Rawluk Against themself	Honorable Senate Finance Committee, Thank you for considering these words when deciding how to vote on SB25-011. I truly appreciate the sponsors' efforts to find solutions to fighting wildfires. This a very important issue for our state. However, please vote No on 25-011. The privacy risks and unintended consequences of a private and closed source deep learning AI connected to cameras, interfacing with satellites, and with a statewide coverage outweigh the benefits, especially given that as it stands, the state would not have an ability for public and transparent audits. Or as an alternative, please continue to amend. The main body of this email is what I've previously sent to other committees, yet I would like to address some of the current amendments. First, There was an amendment to require the blurring of privately owned structures using pixelation or another technology. This is a good step, but I would ask that this committee considers requiring the full lot lines of a private property be pixelated, with a provision that if smoke is detected above the private lot, then this pixelation could then be reduced to the private structure, so as to be able to assess the smoke and potential fire. Additionally, there should be a requirement to pixelate all people, as well as vehicles so as to not inadvertently capture license plate information. Pixelation of schools. Second, the other amendment of note is the inclusion of CRS 18-7-801 Criminals Invasion of Privacy. This is only a class 2 misdemeanor. There are stronger privacy laws that should be contemplated in this bill. Additionally, how would a private citizen ever be aware that there were photos of them being taken maliciously by a third party? The suggestion below of a citizen watchdog portal becomes ever more important when considering the possibility of these pictures taken of citizens on their own private land, potentially sunbathing by their pool for example.

	I would ask that any vendor would be considered to be a State Actor. The litmus test in Manhattan Community Access Corp v Halleck is: 1. A private party that performs a function that is traditionally and exclusively performed by the state. 2. The state directs or compels the private party's conduct. 3. The private party acts jointly with the government Given the test above, it is reasonable that the vendor be considered a state actor in this bill, and as such please add in the ability for a citizen or media to file CORA requests for the imagery collected by the vendor. Also, it would be wise for there to be a public list of all entities with access to the imagery. Third, I would ask that there be an amendment to prohibit any " off-label" use, such as law enforcement, zoning enforcement, assessment of whether a property has dead vegetation, etc. Fourth, I am very concerned that this bill could be funded by gifts or grants. Pano AI for example has done several rounds of funding. They could potentially self finance these cameras as a proof of concept model for future contract procurement. They could self fund, and then raise the price for the live feeds to cover costs. https://agfundernews.com/pano-ai-raises-17m-growth-round-to-expand-its-wildfire-detection-technology They could also solicit funding from NGO's such as the World Economic Forum, which awarded Pano AI first place in the Trillion Trees Competition. Indeed the CCO was inspired to fight wildfires at the 2020 Davos conference, and has since returned to Davos in 2024 to discuss the success of Pano AI on three continents. https://www.globenewswire.com/news-release/2023/01/17/2590234/0/en/Pano-AI-selected-as-a-winner-of-the-2022-World-Economic-Forum-s-Trillion-Trees-United-States-Challenge.html https://www.linkedin.com/posts/asatyam_wef24-ygl24-ygl20years-activity-7155981625124691969-IQoT/ Does Colorado truly want to take the risk of third party funding, and by extension, third party influence?

	Fifth this business model creates a situation where a private company is funded (or self funded) to surveil the state, and the various government agencies are the subscribers to the end product. The government will not have the ability to inspect the process, or to perform code audits on the proprietary AI. Thank you for the consideration of these additional amendment ideas. What follows is the main email I have sent previously, as it is all applicable: From February 2025: Thank you for your decision to remand this bill to the sponsors to fix the issues the Committee highlighted. However, the business model has been implemented in several counties in Colorado, plus in CA, WA, MT, and ID. I'm not sure if Pano.ai or any other company would be willing to make meaningful changes to their transparency policies and business models at this juncture. The model is 24/7 surveillance that requires a 360 degree panorama every minute. This is quite different than some of the more directed technologies that Lockheed Martin proposed such as specific MMA missions over areas with lightning activity. Unfortunately, the bill for Lockheed Martin was voted down in committee this year. National Security: This technology and business model could be a potential national security threat. The state would not allow, but require a statewide coverage of these cameras, as well as monitoring feeds for aerial assets and such, triangulate fires with multiple camera angles, etc, and this is all to be done by a third party with zero transparency besides ISO 27001. Please consider the potential for these cameras to unwittingly see military installations, Low level military training routes for aviation assets, and any training exercises that may be occurring in the mountainous areas. For instance, Eagle Vail Airport is home to HAATS: https://www.cpr.org/2019/09/03/the-eagle-county-airport-is-home-to-one-of-the-countrys-most-unique-military-flight-schools-welcome-to-haats/ There is also concern from the Federal level regarding land ownership near military installations:

	https://www.reuters.com/world/us/us-treasury-expand-security-reviews-land-deals-near-military-bases-2024-07-08/ These cameras, if hacked, could provide a bad actor to have access to information without buying land as described on the article above. Has Pano been vetted by the DoD, DHS, etc for any national security threats? Do their employees undergo full background checks? Will Pano.ai and other who use a deep learning network allow for audits of their systems, and for any potential for unauthorized users to gain access? Citizen Privacy Suggestions: I discussed Pano.ai (one of the largest of such companies) with my friend in cybersecurity and he had these thoughts: About Pano: • Trying to make firefighting reconnaissance like military reconnaissance • Early detection saves money and lives • Pano is using modern day SaaS alerting tools including text, email and live video. • Cameras see 10-20 miles plus zoom. They spin 1 revolution per minute to detect smoke using ai • Once detected a live feed is created in alerts and swift action can be taken • Prescribed burning is an important tool and the realtime monitoring and detection of spot fires is critical to allow for prescribed burning to be safe • Good anecdotes already on effectiveness of catching fires early with Pano Suggestions to ensure citizen privacy: • No expectation of privacy in public but Pano must promise to keep the humans in the video blurred at all times (aka “data minimization“). • This blurring must be done before data is streamed to Pano customers and needs to be done in such a way that it does not impede the quality of smoke/fire protection. • Must not allow any facial recognition to be used and this must be explicitly banned in their contract with all customers. • If a customer finds a human not blurred in the video then they must promise to not use facial recognition to determine the identity of the person and this must be explicit in the contract.

	• Must keep data encrypted at all times (over the wire and while stored). • May want to allow 3rd parties to verify data is not misused and provide a report to customers. • Should publish ethical use guidelines for the data. Third Party audits: I expressed the concerns above to Sen Daugherty, and she had replied that Pano.ai uses ISO 27001 to ensure privacy. I again consulted with my friend in cybersecurity and he replied with this: "Yes, adhering to ISO 27001 helps with data privacy and protection, but it's important to understand how it fits into broader privacy frameworks. ISO 27001 is an internationally recognized standard for information security management systems (ISMS), focusing on establishing, implementing, maintaining, and continuously improving an organization's security practices. Here's how ISO 27001 supports data privacy and protection: 1. Comprehensive Security Framework: ISO 27001 provides a structured framework for managing sensitive information, ensuring that data is protected against risks like unauthorized access, disclosure, alteration, or destruction. 2. Risk Management Approach: The standard emphasizes identifying and mitigating security risks, including risks to personal data, which aligns with data protection principles in privacy laws (such as GDPR and CCPA). 3. Data Access and Control Measures: Adherence to ISO 27001 ensures robust access controls and role-based access, essential for protecting personal and sensitive data from unauthorized handling. 4. Continual Improvement and Compliance: The ISMS model promotes regular auditing and improvement, which keeps data protection practices up to date and helps organizations stay compliant with changing privacy regulations. 5. Alignment with Privacy Laws: Although ISO 27001 is not a privacy-specific standard, its security principles overlap with many requirements in privacy laws. Organizations can pair ISO 27001 with ISO 27701, a privacy information management system (PIMS) extension, which more directly addresses privacy regulations by building on ISO 27001. In summary, ISO 27001 strengthens data privacy and protection by embedding security best practices and a risk-based approach but works best in conjunction with privacy-specific standards like ISO 27701 to fully address personal data protection requirements."

	Additionally he and I discussed that a lot of their camera tech is proprietary, and their AI is also proprietary (would Colorado be able to conduct code audits to ensure safety and privacy?) When I looked further into the ISO situation, I also found that ISO 27090 (Cybersecurity - Artificially Intelligence- Guidance for addressing security threats and failures in AI systems) is still under development: https://www.iso.org/standard/56581.html This standard, once completed, would also seem important for a company with the scope of Pano AI or others in this field. However, actual transparency would be best. Real Estate Considerations: Will having a view of a mountain now reduce property values? Will there be a need for disclosure of where such cameras are in relation to your prospective new home, and whether or not there is Line Of Sight to the camera? Let's consider this potential home privacy issue further: The US State Department has published this risk management profile: https://www.state.gov/risk-management-profile-for-ai-and-human-rights/ This section seemed interesting: "When used in a rights-respecting manner, AI can propel technological advances that benefit societies and individuals, including by facilitating enjoyment of human rights. However, AI can be applied in ways that infringe on human rights unintentionally, such as through biased or inaccurate outputs from AI models. AI can also be intentionally misused to infringe on human rights, such as for mass surveillance and censorship. International human rights are uniquely valuable to AI risk management because they provide an internationally recognized, universally applicable normative basis for assessing the impacts of technology. However, human rights are not always familiar to those involved in AI design, development, deployment, and use, and there is a gap in translating human rights concepts for technologists."

	From the GOVERN section: "Establish and incorporate algorithmic impact assessments, privacy impact assessments, and human rights due diligence processes as part of their organizational risk management processes (Govern1.4). As reflected in the UNGPs, businesses should set up procedures for human rights due diligence, including assessing actual and potential human rights impacts, integrating and acting upon the findings, and tracking outcomes, where more significant risks are prioritized. This includes establishing access to remedy in the event of adverse impacts." Would it be possible for Colorado to require these practices of Pano AI in a transparent and public format? Additionally, we have seen examples of unintended consequences with the implementation of new technology. Hackers have been able to gain access to systems from home security to municipal water systems. This section of the State Department publication would help address this concern: "Assess the likelihood and magnitude of known and foreseeable negative impacts and limitations related to both intended and unintended uses of an AI system (Map 5.1), including potential infringements upon human rights. Consider context-specific deployment environments and how they could lead to different sets of risks (e.g., risks created in conflict settings). When documenting potential beneficial uses and impacts (Map 1.1), include unintended downstream harms that may arise, such as privacy harms from data collected without consent, data re-use, or chilling effects on freedom of expression or freedom of peaceful assembly and association upon individuals or members of groups." Pano AI is unique in that it is being used over vast areas of land. Besides a third party audit with potentially private results, what measures could be considered to enhance public trust and safety, and what could help with Tenant 3 of the AI Bill of Rights? This is a good slide deck that helps break down the types of threats to AI systems as well https://www.snia.org/sites/default/files/SSSI/CMSS24/CMSS24-Hibbard-Security-and-Privacy-Concerns-for-AI%20%281%29.pdf Also, if the American Privacy Rights Act becomes law, would this apply to Pano AI?

Similarity to Drone surveillance:

When it comes to proprietary camera and surveillance, I would ask if cameras on high towers with a vantage point similar to a drone or low flying aircraft would fall under the the aerial surveillance doctrine or something similar?

On page 15, this legal analysis discusses a case where it can be considered to violate privacy if the surveillance is done from public airspace with commonly available technology, but didn't rule on technology inaccessible to the public.

When looking at Pano, their technology is currently proprietary. Are the towers considered to be in public airspace?

https://jlsp.law.columbia.edu/wp-content/blogs.dir/213/files/2017/03/48-Matiteyahu.pdf

To read further:

https://en.m.wikipedia.org/wiki/Aerial_surveillance_doctrine#:~:text=The%20aerial%20surveillance%20doctrine%20is,Unmanned%20aerial%20vehicle%20(UAV).

The aerial surveillance doctrine is the legal doctrine in the United States of America that under the Fourth Amendment, aerial surveillance of an individual's property does not inherently constitute a search for which law enforcement must obtain a warrant. Courts have used several factors–sometimes only one or a few, other times many or all of them–to determine whether the surveillance in question is a search in violation of one's constitutional rights: the object of the surveillance (whether it's commercial property or an individual's home or curtilage), the technology employed (whether, on the basis of its capabilities, it simply enables "naked eye" observations or allows the user to acquire otherwise unobtainable information), the duration of the surveillance, scope of aggregated information (whether it's limited or extensive in nature), and the vantage point from which the surveillance is conducted (whether it's from a place that one can reasonably expect to be observed).

In Summary:

	In summary, we are asking a private company to surveil the state, and then the state or local agencies have to subscribe to buy the information. There is no citizen watchdog group that can see what is actually being learned by the closed source AI. This could very well violate Carpenter v US. Additionally, the Institute for Justice has a lawsuit against Norfolk VA for Flock Safety ALPR, as they could very well constitute a search under the 4th Amendment, as they could be considered a state actor while working with a public agency, and they store information for more than the 7 day litmus test that was ruled on in Carpenter. How long does Pano.ai and others store their information? What does the deep learning AI gain from this data? In the end, Sonia Kastner said in the My Climate Journey podcast, that Pano did a gap analysis between military surveillance tech, and what is commonly available to firefighters, and that they are working to close that gap. A private company with that type of tech, that type of reach, and that level of opacity should never be embraced in a free society. Additionally, the unlimited number of back end users is concerning as well, when one considers mission creep. https://mcj.vc/inevitable-podcast/pano-convective-capital This tech will evolve faster than we can imagine, and the uses will grow exponentially. Not all uses of this tech will be in favor of a free society, Thank you, Mike Rawluk