Members of the Joint Committee on Information Management and Technology:

I support the creation of the Task Force on Artifical Intelligence (AI). This task force is critical for identifying how we can make the most out of AI while ensuring Oregonian's are protected and not taken advantage of.

I am also here today to ask that two more positions be added to the task force: a cybersecurity expert, and an AI red-teaming specialist. These security specialist positions are critical to understanding how to address the gaping security hole that AI is creating for consumers and businesses across the state.

I am hopeful that the following interrelated problems could be addressed by the task force, or by the Joint Committee:

1. Social Media platforms, including TikTok, Youtube, Facebook, and Instagram, are replacing the feed and ad recommendation engines with AI. This is wreaking havock on our society at large, especially on our young people. An AI that knows everything you've seen, commented, and liked is able to draw you in even further with "engaging" content. This may lead a young teen interested in healthy eating to be fed more and more extreme content, until they are being shown videos on annorexia. Oregonians must have a right to control the algorithm/AI which supplies their feeds, and parents must be given the ability to "opt-out" of AI-controlled feeds for their children under the age of 18.

2. Companies around the globe are now using our data to train their AI tools, and we have simply handed it over without a question. With a few exceptions, we have not seen a large-scale class action lawsuit on whether the AI tools that are being commercialized are even legally allowed to use our data under the Creative Commons License. At the very least, we must give Oregonian's the right to "opt out" of having their data be used for training AI tools, including publications, photos, and data on public websites.

3. Impersation of people and their likeness is easier now than ever with the use of Generative Adversarial Networks (GANs), which are being used to create false images and recordings of anyone from world leaders to loved ones. While industry has joined together to work toward a "digital watermark [1]" to ensure provenance of AI generated media, we must be vigilant in educating Oregonians on how these AI tools may be used to produce "fake" media, and have even been used to scam people and steal identities.

4. AI Large-Language Models (LLM's) are easily fooled due to their non-deterministic design, which makes them a great target for malicious state actors. As most LLM's are trained on a corpus of internet web ages, this can lead to very misleading "facts" being generated. We must not only educate Oregonians about the "hallucinations" that LLM's frequently display, we must ensure that companies display public "potential false information" notices to consumers when results are AI generated by an AI.

5. AI LLM's are increasingly being integrated into every consumer and enteprise tool at an alarming rate for fear of being "left behind," and hackers and bad actors are having a field day. With the integration of AI as "plug-ins" to other tools, there is a gaping security hole for hackers to pursue. Similar to a grade you might recieve from the health department for a restaurant, a "Data Protection Grade" should be mandated for products and "AI plug-ins" to ensure proper data protection standards have been implemented, and that AI/LLM's have been properly grounded and sandboxed to protect against prompt injection and data exfiltration attacks.

While I am excited about the potential for AI, I am deeply concerned at the rate of adoption of these tools and technologies and how they are being used without concern for consumer protection, data privacy, provenance, and security. I am excited for the day when AI tools can assist with making our businesses and governments run more efficiently and deliver better products and services. **I humbly request that two security professionals are added to the task force to ensure we adopt a resposible approach to AI adoption in our state.**

Sincerely,

Richard "RJ" Sheperd (Portland, Oregon)

1. Coalition for Content Provenance and Authenticity, c2pa.org.