



May 24, 2024

The Honorable Mark R. Warner, United States Senate
703 Hart Senate Office Building
Washington, DC 20510

Dear Senator Warner:

We received your letter of May 14 regarding the Tech Accord's efforts concerning AI, including potentially deceptive uses in the 2024 elections. Your staff was provided with a less formal presentation of our answers to your individual questions on May 24 as you requested, which generally summarizes the key points below.

AI certainly is increasing the volume and complexity of the threat landscape at an unprecedented pace, and we're pleased that members of the U.S. Senate are understanding and prioritizing these issues and taking an interest in the ideas and efforts of Tech Accord member companies.

Trend Micro is exclusively in the business of cybersecurity, having started the original anti-virus business in 1988, and now operating in more than 65 countries as one of the largest cybersecurity providers. Prevention of impersonation and verification of provenance are key aspects of cyber-defense, and Trend's mission statement of "making the world safe for exchanging digital information" is also indicative of our envisioned use of AI. I will address your questions more specifically below, mapped to the question numbers from your letter:

1. Trend does not create products for content generation. Our products are designed to detect, prevent, and mitigate attacks by bad actors. Though security is a broad area, covering various layers and methods, detection of impersonation (spoofing, phishing, BEC) and identity, provenance, or chain of custody type verification (SSL, code certificates, RFID, etc.) is a critical aspect of security that is being improved by AI. In that sense, there is an AI "arms race" of sorts where the exponential proliferation of attacks enabled by AI requires AI powered security to effectively counter, and the use of AI in our products serves to actually combat the risks under discussion here.
2. Trend regularly blogs about threat actors' use or potential use of AI (including generative AI) based on work done by our global research team. Our blogs are read by thousands of individuals around the world and we translate them into multiple languages to extend their reach. A few examples:
 - <https://www.trendmicro.com/vinfo/us/security/news/threat-landscape/navigating-the-threat-landscape-for-cloud-based-gpus>
 - <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/back-to-the-hype-an-update-on-how-cybercriminals-are-using-genai>
 - https://www.trendmicro.com/en_us/research/24/e/poll-security.html

Trend Micro Incorporated

225 E. John Carpenter Freeway, Suite 1500, Irving, TX 75062, USA
trendmicro.com



- https://www.trendmicro.com/en_us/research/24/b/earth-lusca-uses-geopolitical-lure-to-target-taiwan.html
- https://news.trendmicro.com/2021/02/24/social-media-in-action-how-does-social-media-combat-election-misinformation/?_ga=2.11368628.1636512739.1716214210-435208103.1682688904

3. Due to our cybersecurity specific mission, we have not created resources specifically for independent media and civil society organizations.
4. It's very unlikely that Trend's products could or would be misused based on AI elements, and Trend's products do not actually create media or other content that may require separate credentialing or authentication. Trend's policy engagement on AI issues has been indirect, and primarily through its board level membership in the Business Software Alliance (BSA) and through the US Chamber of Commerce.
5. Trend is soon releasing a new tool (initially for commercial customers) which is designed to detect deepfake video content.
6. Trend does not offer social media or content distribution platforms.
7. Trend does not offer social media or content distribution platforms.
8. Although Trend does not offer generative AI products, but instead offers products that help to prevent impersonation by bad actors (along with other forms of attack), we do use generative AI to help customer SOC analysts improve their workload and threat hunting capabilities. In this case AI is being used to counter the security threats which may even be AI related, but any generative AI element of the service does not include deliverables to the customer where identity, provenance, authorship, IP or similar issues are relevant to the customer when separated from the security aspect.
9. Although Trend does not offer social media or content distribution platforms, we are potentially open to participation in information sharing programs concerning machine generated false and/or malicious content.

I hope that these responses have addressed your concerns and helped to clarify the nature of Trend's utilization of AI in its products.

Best Regards,

DocuSigned by:

Felix S. Sterling

A3F077256243465...

Felix S. Sterling

Chief Legal Officer & EVP Global Policy and Compliance

Trend Micro Incorporated

225 E. John Carpenter Freeway, Suite 1500, Irving, TX 75062, USA

trendmicro.com



Trend Micro Incorporated

225 E. John Carpenter Freeway, Suite 1500, Irving, TX 75062, USA
trendmicro.com



Trend Micro Incorporated

225 E. John Carpenter Freeway, Suite 1500, Irving, TX 75062, USA
trendmicro.com