

McAfee

6220 America Center Drive
San Jose, CA 95002
McAfee.com



June 4, 2024

The Honorable Mark R. Warner
United States Senate
Washington, DC 20510

Dear Senator Warner,

Thank you for your recent letter requesting McAfee's response to the commitments made as part of the Tech Accord to Combat Deceptive Use of AI in 2024 Elections. Election security is a critical issue that McAfee has been committed to supporting globally for many years. McAfee has also been a leader in researching and protecting customers from the risks that AI technology can pose. We applaud your leadership in these two areas and welcome the opportunity to share more information about our efforts.

Given the importance of these issues and our commitment to ensuring that consumers are able to safely live their digital lives, we enthusiastically signed the Accord in February of 2024. Our role in this space differs from most other signatories. While we leverage AI in our products, we are not a company that distributes general-purpose AI tools, nor are we a platform for the distribution of information that could potentially be altered through the use of generative AI. Rather, we are a cybersecurity company; our mission for over 35 years has been to protect people's electronic lives.

Moreover, we have long believed that election security is an important part of this mission. For example, as you may know, prior to the 2018 election cycle, McAfee conducted [original research](#) exploring the possibility of election site spoofing and phishing attacks in which malicious actors could take over websites of local boards of elections or create fake alternative sites that could fool voters. This research led to briefings on the topic with officials from CISA and NSA, as well as local election officials. Ultimately, McAfee's work helped inform [guidance from CISA](#) and others about the need for election offices to use the .gov domain for their sites.

Meanwhile, the introduction of and increased access to sophisticated artificial intelligence tools has been an exciting inflection point and, in many ways, a beneficial addition to our daily lives. However, as with any technological advancement, these same tools, when leveraged by malicious actors, have significant impact on the threat landscape. [Recent research conducted by McAfee](#) showed that the vast majority (72%) of American social media users find it difficult to spot AI-generated content such as fake news and scams. In fact, the weaponization of AI is something that McAfee researchers and leaders [publicly identified](#) and began investing resources in as far back as 2019.

Our teams are actively researching and developing tools to combat deceptive AI and deepfakes, including McAfee's Deepfake Detector, a product that we expect to release soon. This is a tool that can alert users when we detect that a video they are watching contains AI-generated content.

We first [demonstrated the technology behind McAfee's Deepfake Detector](#) (then known as Project Mockingbird) at the 2024 Consumer Electronics Show this past January. Using a combination of detection models powered by our own AI models, this technology analyzes audio content and identifies whether or not recorded audio has been generated using artificial intelligence. We have focused on audio first as cloning voices of public figures, candidates or trusted media personalities and overlaying them onto generic video footage is currently the fastest and easiest way to create convincing deepfakes.

Beyond our products, McAfee has long committed to helping educate the broader public on a wide variety of cybersecurity and online protection issues, including [election-related deepfakes](#). We regularly publish articles, blogs, and news releases on these topics on our website. We have a [news hub](#) specifically designed to highlight AI scams and other news related to AI, and we are developing more detailed content to alert people to high-profile deepfakes, whether election-related or otherwise. In addition to our own content, we also regularly engage with news outlets to provide expertise and help spread awareness on these issues (see, for example, a recent [WIRED article](#) focused on tips to protect individuals from falling victim to AI scam phone calls). We are also exploring opportunities with news and media partners to find ways to leverage our Deepfake Detector and other technology directly in those spaces to help partners identify deepfakes or otherwise protect news content integrity.

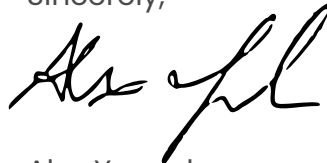
The use of generative AI by both good and bad actors is a rapidly evolving situation with new and more advanced tools being introduced at a lightning

pace. McAfee is committed to using both traditional and AI technologies as well as consumer education to fight the malicious uses that impact not only the upcoming and future elections, but every day digital lives.

If you would like to further explore any of these topics or learn the latest about McAfee's activities, we are happy to arrange a meeting.

Thank you once again for requesting details of McAfee's initiatives to protect elections from deceptive AI tactics. We are all in on this critically important issue and will continue our efforts to explain and develop technology as well as help consumers navigate the complex landscape they face, especially as November approaches.

Sincerely,



Alex Yacoub
Legal Director, IP, Product, and Brand
McAfee