Chairman Blumenthal, ranking member Hawley, Senator Klobuchar, and committee members: I thank you for your stated concerns on the impact deepfakes have on our elections, on our democracy, and on society, and I thank you for holding this hearing, as well as requesting my presence here. It is an honor to provide any insights that may be of help to both your committee and the American people, and I applaud the committee's great efforts in surfacing the deepfake problem in front of the nation.

Over the last two years, there has been an air of excitement and wonder over the many rapid technological advancements and developments in what we now call generative artificial intelligence. Such advancements are now very much a permanent fixture in society, in conversation, and at work, and are slowly becoming just as prevalent as other technologies that were once novel but are now commonplace in our everyday lives. As a longtime cybersecurity official, myself and my team at Reality Defender foresaw the emergence of such technologies into the mainstream well before this happened, and were demonstrably early in working to thwart them before they were an equally mainstream issue. In fact, we built our company because we've seen the tangible impacts that weaponized content and disinformation had on our loved ones, and we sought to stop what are now the most advanced disinformation-driven threats of our time.

Generative artificial intelligence, or Generative AI, is not a fad, nor is it an entirely negative presence in our world. AI, and to a lesser extent generative AI, has been used for many years, largely in the background without the fervor and publicity it gets today. Thanks to the rapid adoption and iteration over the last several years, led largely by the unmatched innovation in American tech companies, we're now privy to concepts that were once works of science fiction.

Myself, my team at Reality Defender, many in the tech world, and many consumers do not feel that *all* generative AI technologies are bad. Far from it. Many uses of this technology can echo the technology that came before it, augmenting human capabilities and increasing the speed of innovation. A hyper-realistic avatar could, for instance, make video calling possible to parts of the country where high-speed internet access is sorely lacking, reducing the need for bandwidth. A chatbot trained on fifth-grade math can not only help a student with their homework, but help them understand how to solve a problem.

There are a million and one incredible and groundbreaking uses for these technologies that will change innumerable lives.

Yet just as generative AI has its immense benefits, so too does it imperil core societal tenets that we hold dear. Deepfakes, the colloquial term for fully or partially AI-manipulated works that seek to mimic existing individuals or create new ones wholesale, are especially troubling in how they can fabricate a new reality for a person or millions of people.

We've seen this on the large scale in recent weeks, with Russian media falsely depicting Ukrainian forces as the perpetrators of the devastating attack in a Moscow music hall, or with the robocall of a fake President Biden to thousands of New Hampshire constituents. This is a

new and precise weapon of propaganda during elections and during wartime, and we are just beginning to see what it can do.

This is a new problem and dangerous problem that is increasing in size, scope, and damage. Our adversaries are getting smarter about how to apply deepfakes effectively to manipulate elections, spread anti-American sentiment, and sow discord.

This is not just a centralized weapon. We see the harms deepfakes, created by a vengeful individual on a smaller scale practically every week, with non-consensual deepfake pornography — over 99% of which depicts girls and women — ruining countless lives of schoolchildren, of notable names, of wives, and of daughters. Even high school students in Baltimore, MD and Putnam County, N.Y. managed to degrade the reputation of their school principal with a high quality deepfake.

I cannot sit here and list every single malicious and dangerous use of deepfakes that has been unleashed on Americans, nor can I name the many ways in which they *can* negatively impact the world and erode major facets of society and democracy. I am, after all, only allotted five minutes. What I can do is sound the alarm on the impacts deepfakes can have not just on democracy, but America as a whole.

Generative AI models and technologies are available to anyone with basic internet access and either a credit card, or, as is often the case, for no money at all. Anyone can create an AI-generated audio, video, image, or text file that, by and large, is so convincing that even our own experts with PhDs cannot manually tell if they are real or fake. What's just as important is how anyone can *distribute* this media on a massive scale thanks in part to the popularity of social media and content platforms. These platforms have all but eradicated their trust and safety teams who would normally prevent abuse and disinformation from propagating to millions. Though these platforms have, with minimal effort, kindly asked their users to self-label content, there are no penalties nor further action if they don't.

Because of the democratization of these technologies, because everyone has access to them, and everyone has access to all publicly available materials on the internet, anyone can deepfake anyone without their consent and spread these deepfakes like wildfire. By anyone, I mean men and women, children and adults, Democrats and Republicans. This is, by and large, a non-partisan issue, and one that both parties should equally fear.

There have been countless attempts around the world — both successful and otherwise — to subvert elections and sway public opinion. This year we saw our Chinese and Russian adversaries test out early deepfake-fueled election interference campaigns in Taiwan and Slovenia, respectively. While these efforts may not have changed the overall outcome of the election, they are a warning we must heed and learn from to protect our own elections.

As these materials appeared and spread to millions in minutes, the research and responses in pinpointing them as deepfakes took hours, if not days to spread to a disproportionately smaller

group. As Mark Twain once said, “A lie can travel halfway around the world while the truth is putting on its shoes.” By the time a deepfake has spread like wildfire, any reporting that calls it a deepfake is already too late and will reach only a tiny fraction of those who first saw it. Determining truth will always be slower and more difficult than spreading a lie.

Now, Taiwan and Slovenia are not America, but the same thing can and has, in election materials, in robocalls, and in campaign affiliate-disseminated memes, happened here. This is not fear mongering, nor is it AI alarmism, doomerism, or conspiracy-minded hyperbole. It is simply the logical progression of the weaponization of deepfakes.

If legislative measures are not expeditiously taken to enforce the proactive and detection of deepfakes where Americans consume content, deepfakes will have a sizable impact on our election this November and every election going forward, with potential negative implications and effects on and for both sides of the aisle.

I applaud the efforts of ranking member Hawley and Senator Klobuchar on their Protect Elections from Deceptive AI Act. Unlike previous measures that have more or less given the pen to the largest content and social platforms, this law could meet any potential threats that deepfakes pose to our elections head-on and have tangible consequences for those seeking to disrupt our democracy with deepfakes — as well as the platforms used to disseminate such materials. Though states like Minnesota have passed measures against specific uses of deepfakes, there are no federal laws regarding the detection or prevention of dangerous deepfakes on the books, and this law would do a world of good in ensuring some uses of deepfakes do not, in fact, impact the coming elections and all that come after.

That said, generative AI moves faster than any technology that preceded it. Legislation needs to not only move at the same speed, but faster, forecasting and potentially anticipating ill-intended consequences that may stem down the line from the latest generative AI technologies, all built by companies who "move fast and break things."

Unlike the apps and startups who followed such a motto before them, the "things" in this instance are aspects of society everyone in this room holds dear. Democracy. Truth. Trusting what you see and hear. It is not a stretch to say these are at stake when any American — any person — can both create mis- or disinformation to convince any other person they are anybody, saying anything, in real time, for free or cheap, and with little to no technical expertise needed.

I am here to say that we must treat deepfakes with equal or greater importance as we do with the worst kinds of content that existed before it, precisely because it gets at the heart of what makes us human and wholly erodes the trust of our political dialogue. I urge our elected officials to mandate the removal and expulsion of such dangerous deepfakes and AI-generated media with complete and total urgency and not, as it currently exists, have social platforms and businesses relegate it to yet another chore and decision for the average American to determine and make. We must mutually agree, as Democrats and Republicans, men and women, that the

deepfake threat is a threat to everyone, to the things we hold dear, and to America itself. And we must act quickly and at the same speed that AI progresses, lest we be taken by surprise by new attacks from afar, from at home, and, most importantly, on truth.