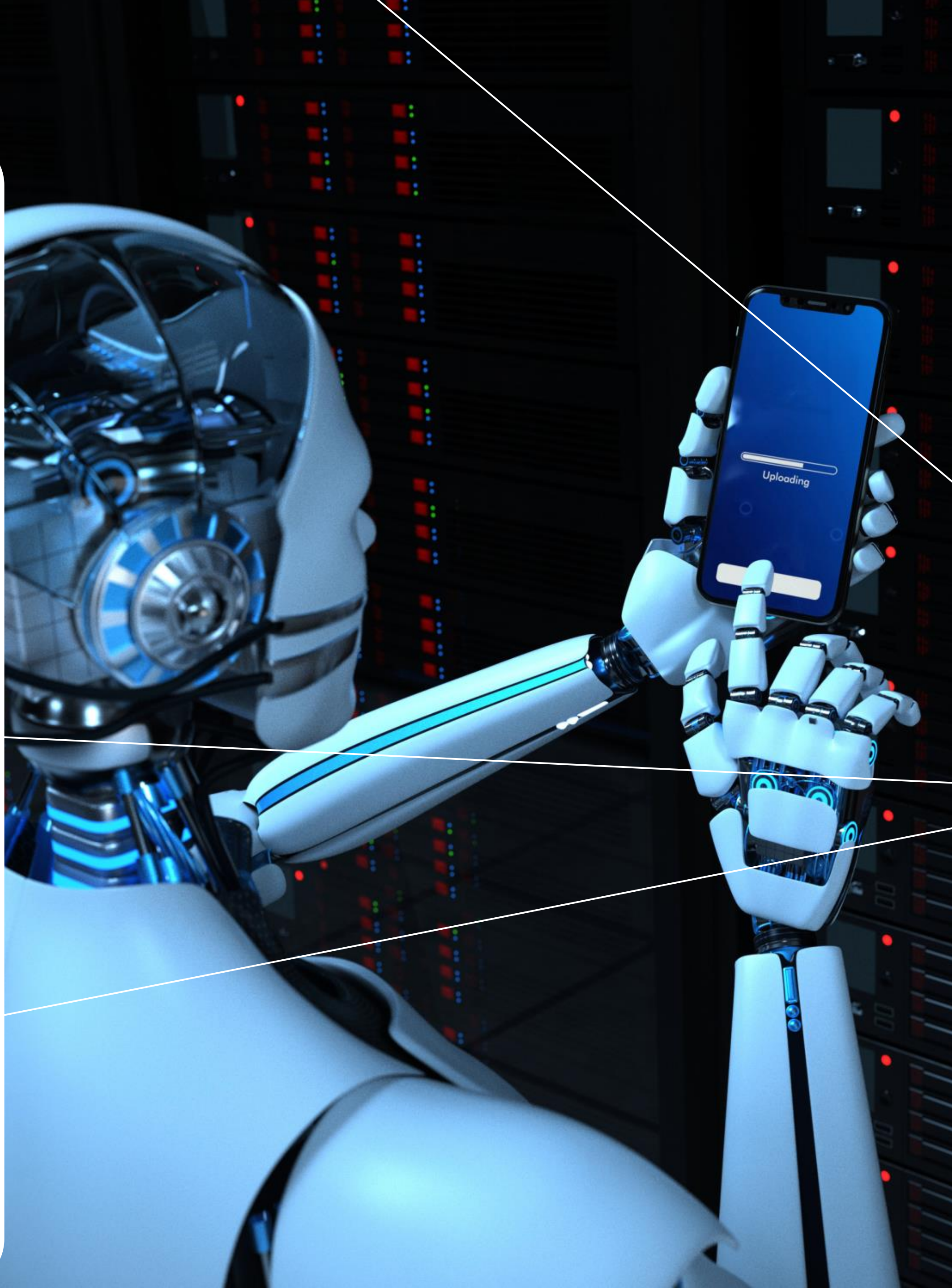
Bad Actors and AI: What's Next?

Greg Bohl

Chief Data Officer, TNS Comms Division

Date: May 6th, 2024



The President of Deep Fakes?

In January, a robocall from "President Biden" went to New Hampshire voters urging them not to vote.

"Voting this Tuesday only enables the Republicans in their quest to elect Donald Trump again. Your vote makes a difference in November, not this Tuesday."

"Joe Biden" in the New Hampshire robocall

How Might AI Impact Political Races?

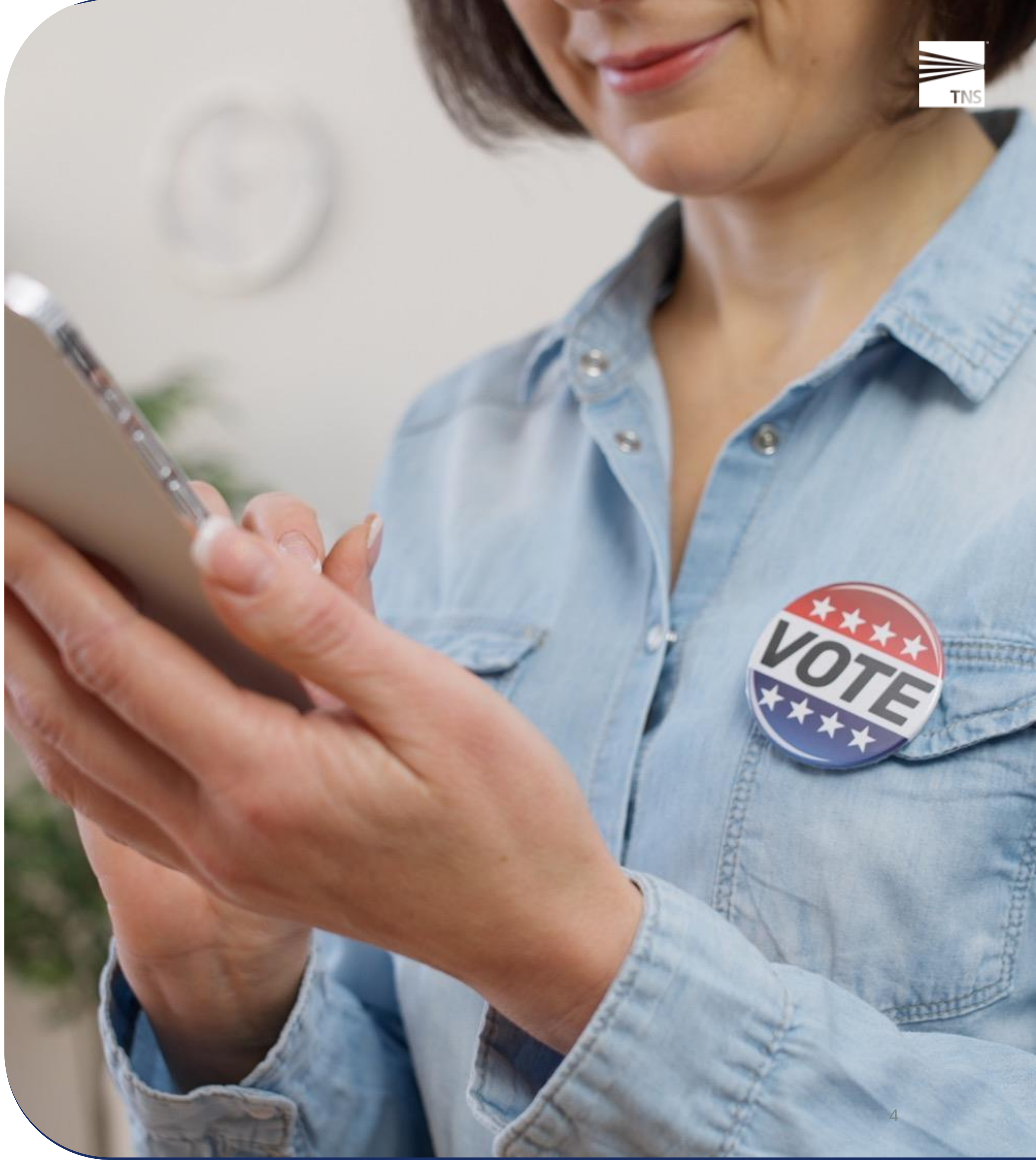
Robocalls are used as a primary communication vehicle during election seasons. The use of AI-generated voices is a real and continued threat.

704,065 The number of political calls in New Hampshire the week before the primary

902,351 The number of political calls in New Hampshire the month before the primary

How Might AI Impact Political Races?

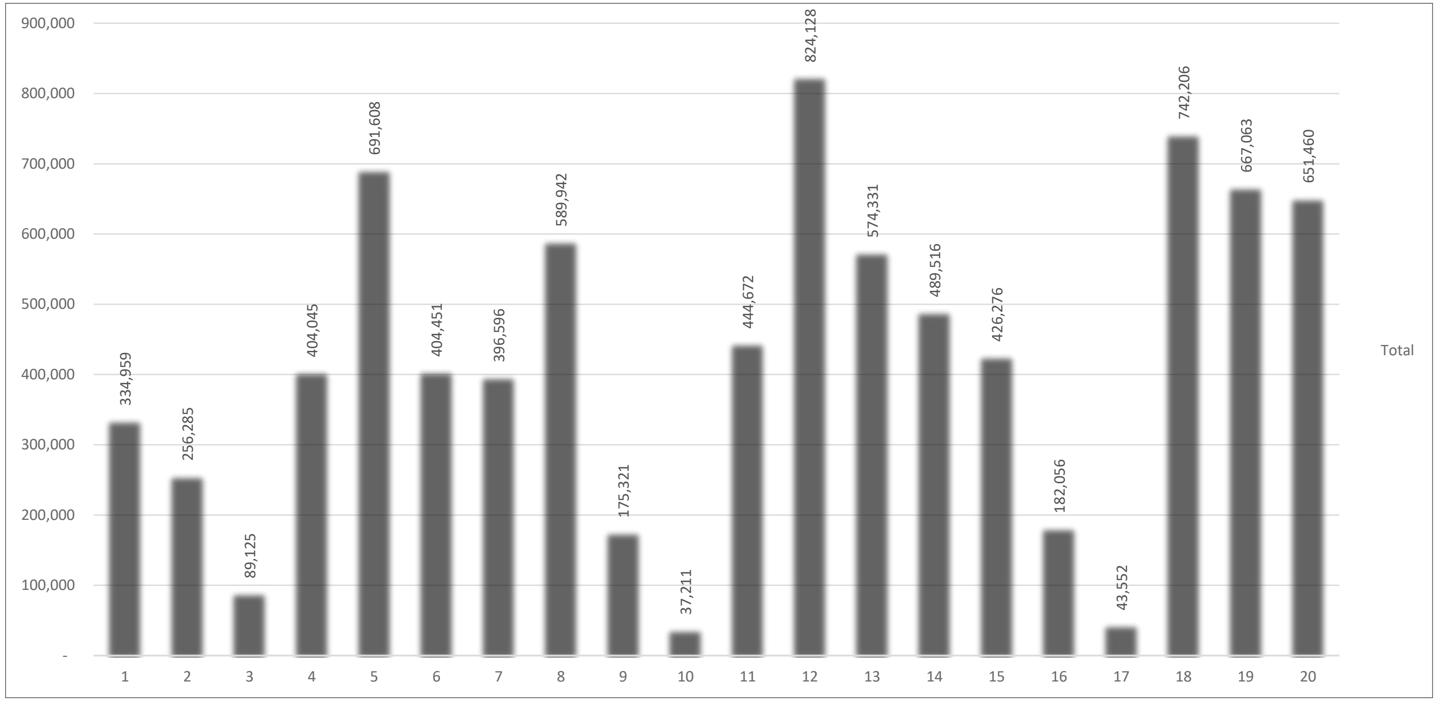
1:1 For registered voters in New Hampshire, that’s nearly a ratio of one to one



How Is the Threat of AI Amplified During Primary Season?

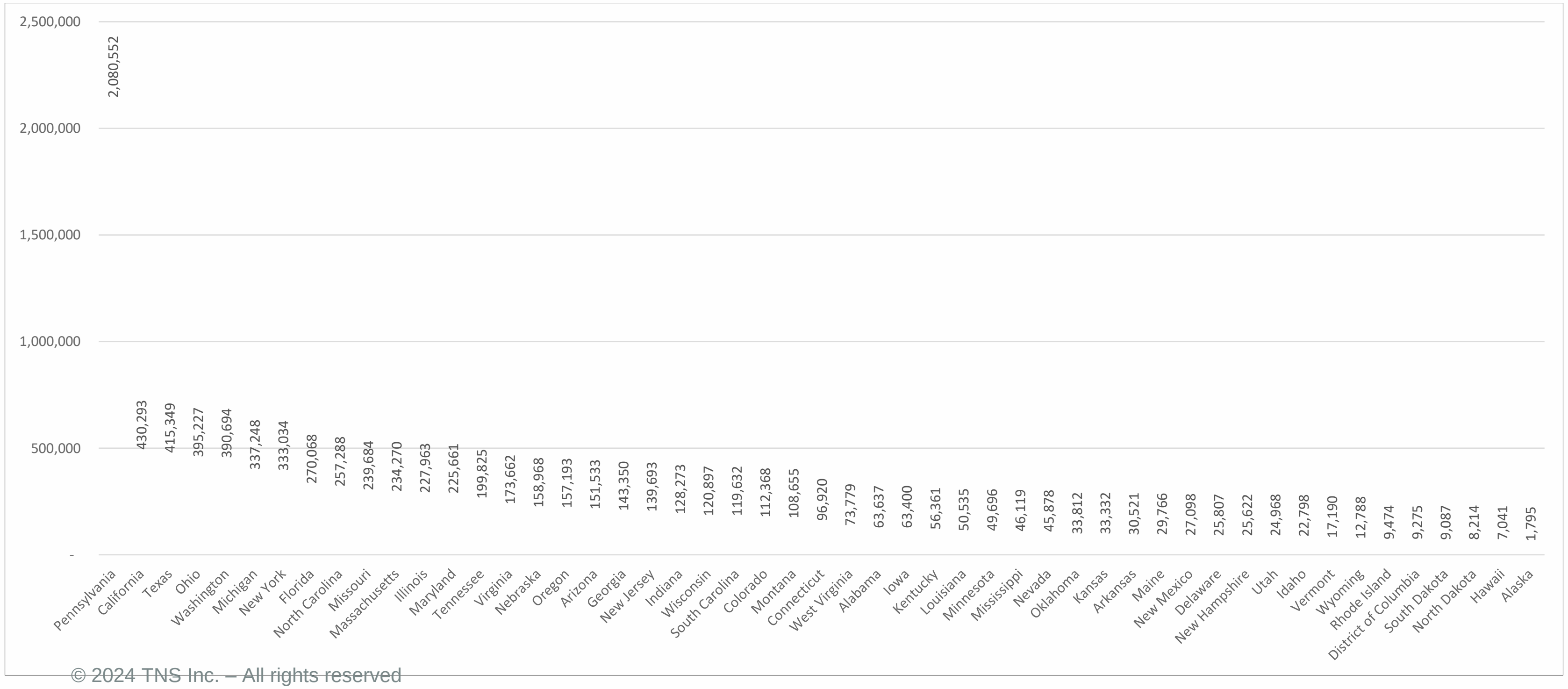
As might be expected, political calls in March, the month of Super Tuesday and other primaries, were particularly high.

Political Call Trends rising per days (March)



How Is the Threat of AI Amplified During Primary Season?

Top States include PA and CA from - March 1st to 20th



Political calls were particularly dense in PA.

Is the FCC Doing Enough?

The FCC ruling impacted political calls. But did it do enough?

“Bad actors are using AI-generated voices in unsolicited robocalls to extort vulnerable family members, imitate celebrities, and misinform voters. We’re putting the fraudsters behind these robocalls on notice.”

Jessica Rosenworcel, FCC Chairwoman

Can Deep Fake AI Be Regulated?

In February 2024, the FCC announced the unanimous adoption of a ruling making AI-generated voices in robocalls illegal.

> "Over the last few months, I've been proud to see our government convene quickly and effectively to explore the implications of artificial intelligence."

Geoffrey Starks, FCC Commissioner

How Is the Government Reacting?

Government reactions have been swift and numerous.

- FCC makes AI voices in robocall calls illegal
- FTC authorizes the use of “compulsory process in nonpublic investigations” regarding AI
- FTC prohibits government and business impersonation schemes to combat AI
- White House releases an Executive Order setting standards on AI

> “With this Executive Order, the President directs the most sweeping actions ever taken to protect Americans from the potential risks of AI systems.”

White House Statement, October 2023

How Are Bad Actors Using AI?

Bad actors leverage generative tools due to the cost and easy access. So what are they doing exactly?

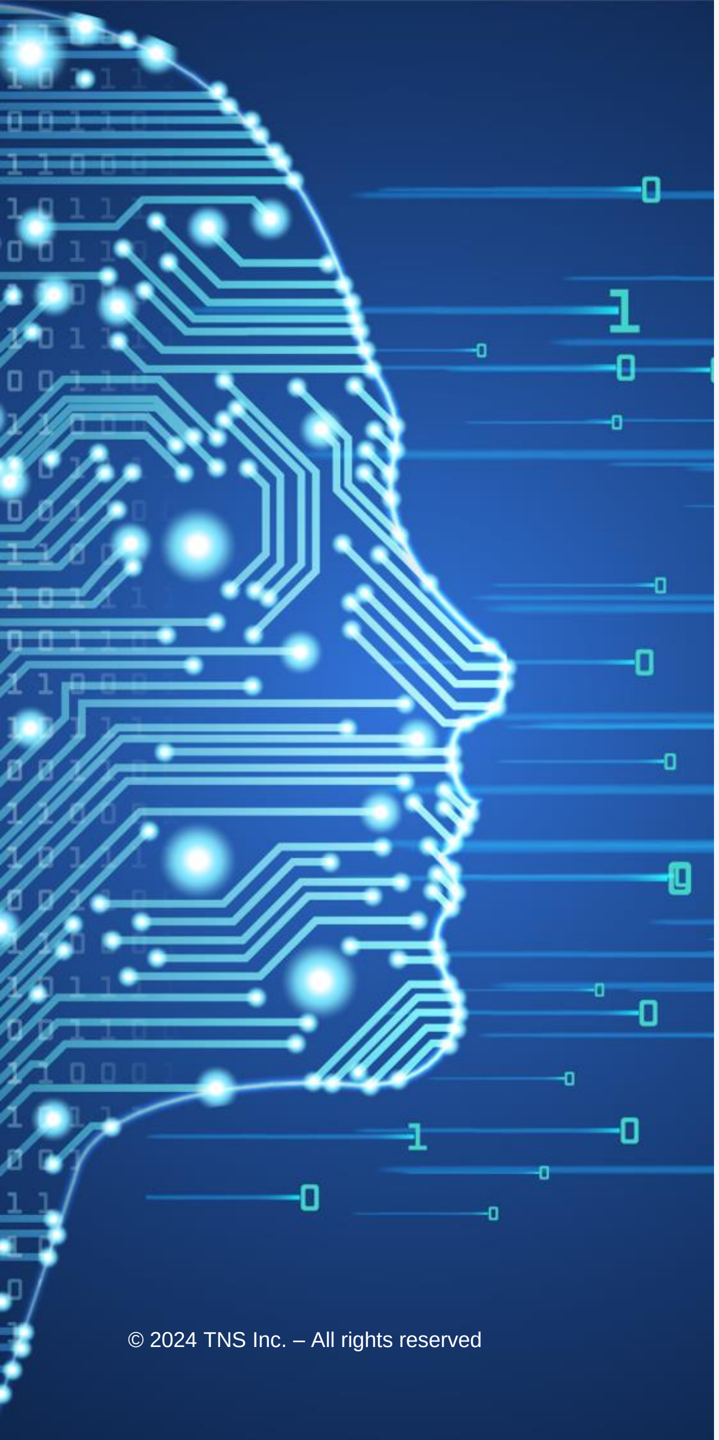
- **Broad Reach**—using deep fakes to replicate politicians, celebrities and other public figures
- **Narrow Focus**—creating a single opportunity using human engineering
    - Commonly uses fear
    - Victims might not have the means to pursue attackers legally
    - Law enforcement has limited bandwidth

© 2024 TNS Inc. – All rights reserved

Will video-calling clones be next?

> “Delphi, touted as the world’s first digital cloning platform, uses data from podcasts, videos, PDFs and other content to develop a clone that can mimic the user’s thoughts and speech—and it can take as little as one hour.”

NY Post, April 2024



What Is a Deep Fake?

Deep fake images, video and voice can be created using inexpensive or free commercially available tools.

- A deep fake image or video is when someone's face or body has been digitally altered so they appear to be someone else, typically to spread misinformation
- A deep fake voice is a synthetically generated voice to replicate someone's voice, including their volume, pace, tone, pitch and enunciation

> "As technology advances, it will become increasingly difficult to identify manipulated media."
>
> Department of Homeland Security Report

Who Should Be Most Concerned About the Use of AI and Deep Fakes?

Carriers

- Require prior consent from the called party
- Should block calls that lack that consent
- Regulations are vague and up to interpretation

Consumers

- AI can harm the user experience but also improve it
- Spam detection must constantly evolve
- Deep fakes create additional challenges that must be faced

Businesses

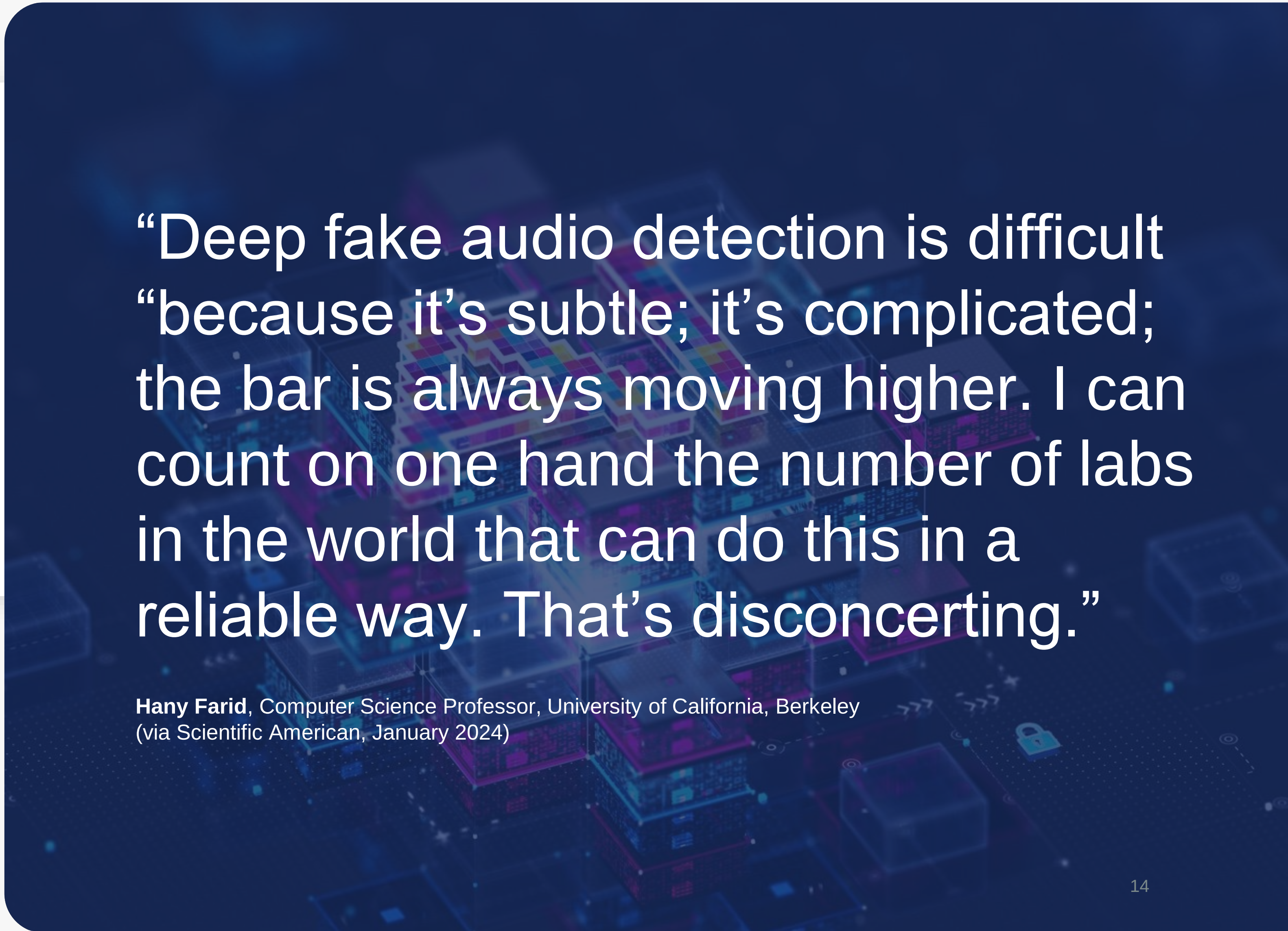
- Tools such as branded calling can build trust
- Branded calling can also slow down bad actors
- Multi-level authentication is also key

> “Board directors and CEOs need to increase their knowledge of Deep Fakes and develop risk management strategies to protect their companies.”

Forbes, December 2023

How Can You Detect Deep Fakes?

Detection depends on identifying ten qualities of a voice and image subtleties omitted by the Gen AI model.



“Deep fake audio detection is difficult “because it’s subtle; it’s complicated; the bar is always moving higher. I can count on one hand the number of labs in the world that can do this in a reliable way. That’s disconcerting.”

Hany Farid, Computer Science Professor, University of California, Berkeley
(via Scientific American, January 2024)

> “A Brooklyn couple got a call from relatives who were being held ransom. Their voices—like many others these days—had been cloned.”

The Terrifying Scam that Uses Your Loved One’s Voice
The New Yorker, March 2024

What and Who Are the Primary Targets of Deep Fake Today?

While everyone is a target, bad actors have targeted certain demographics more than others.

- Voters
- Pre-teens, Teens
- Senior Citizens

What Are Some Common Sense Things We Can Do Today?

TNS has reported several steps individuals and businesses can take to protect themselves.

- Change voice mails to a neutral voice
- Create a family-safe word
- Use a secondary safe word in messaging apps like FaceTime and WhatsApp

> “While deep fakes provide a new terrain in the battle against misinformation and defamation, you can take proactive measures to protect your digital identity.”

National Cybersecurity Alliance

In Summary

01 Regulatory is catching up, but it still has a way to go

02 Bad actors will always be at the forefront of technology

03 Commercial efforts are necessary to comply with regulatory changes

04 AI is still in its infancy—new solutions will always be needed