ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Testimony of

Daniel Castro
Vice President
Information Technology and Innovation Foundation

Before the:

Senate State Affairs Committee
The Alaska State Legislature

Hearing on:

"AI, Deepfakes, Cybersecurity, and Data Transfers"

February 1, 2024

INTRODUCTION AND SUMMARY

Chair Kawasaki, Vice Chair Claman, and members of the committee, thank you for the opportunity to share feedback on Alaska Senate Bill 177, a legislative proposal concerning deepfakes in elections and the use of artificial intelligence (AI) by state agencies.

I am the vice president of the Information Technology and Innovation Foundation (ITIF). ITIF is a nonprofit, nonpartisan think tank whose mission is to formulate and promote public policies to advance technological innovation and productivity. I am also the director of the Center for Data Innovation, a research institute at ITIF focusing on the intersection of data, technology, and public policy.

In my testimony, I would like to describe how your committee can address the risk of deepfakes in elections and misuse of AI in government without penalizing legitimate uses of AI. Striking the right balance will be essential to address public concerns while not unnecessarily constraining the beneficial uses of this emerging technology.

DEEPFAKES IN ELECTIONS

Policymakers are rightfully concerned that bad actors will exploit advances in generative AI to create realistic media that appears to show people doing or saying things that never happened—a type of media commonly referred to as "deepfakes." Deepfakes have the potential to influence elections. For example, voters may believe false information about candidates based on fake videos that depict them making offensive statements they never made, thus hurting their electoral prospects. Similarly, a candidate's reputation could be harmed by deepfakes that use other people's likeness, such as a fake video showing a controversial figure (e.g., Andrew Tate or Jeffrey Epstein) falsely supporting that candidate.[1] Finally, if deepfakes become commonplace in elections, voters may simply no longer believe their own eyes and ears, and they may distrust legitimate digitial media showing a candidate's true past statements or behaviors.

One way to address this risk is by updating state election laws to make it unlawful for campaigns and other political organizations to knowingly distribute materially deceptive media that uses a person's likeness to injure a candidate's reputation or manipulate voters into voting against that candidate without a clear and conspicuous disclosure that the content they are viewing is fake. Such a requirement would prevent, for example, an opposing campaign from running advertisements using deepfakes without full transparency to potential voters that this media is fake.

However, legislators should understand that there are limits to what a transparency law on deepfakes can achieve. Election laws can ensure that all legitimate political organizations play by the same set of rules, or if they fail to abide by those rules, face certain penalties. However, they do not stop certain bad actors, such as foreign adversaries, who knowingly engage in illegal activity but are beyond the reach of domestic laws. Nor will these types of laws stop First Amendment-protected free speech (e.g., parody, satire, criticism, etc.) by voters that is uncoordinated with any political organization, such as a teenager posting a deepfake about a candidate on social media.

State lawmakers should create transparency requirements for deceptive media in elections that adhere to the following principles:

- **Treat AI And Non-AI Fake Media The Same**: While advances in generative AI have made it easier to produce deepfakes, there are techniques that do not involve AI that can create similar results. For example, a talented impersonator can produce a realistic audio clip of a candidate speaking and, with the right makeup and prosthetics, create a convincing photograph or video (e.g., actor Tina Fey impersonating Sarah Palin). Similarly, a campaign may use AI to alter photographs of a candidate, such as to make them appear older or younger, slimmer or heavier, darker or lighter skinned—or they could use non-AI photo editing tools to achieve the same effect. Legislation should apply the same rules to all deceptive media, regardless of whether it is produced with AI.
- **Allow Beneficial Uses of AI-Created Content:** Most software tools to create and edit digital media are quickly integrating AI. Increasingly, even basic photo, audio, and video editing will involve the use of AI. For example, a campaign may use AI to produce videos of their candidate answering questions more efficiently rather than having the candidate record their answers directly. Or a campaign may use AI to produce videos of their candidate speaking in a language that they do not speak to communicate better with more voters. In many contexts, these use cases are reasonable and appropriate when done with the candidate's consent. Therefore, lawmakers should avoid creating rules that are too broad that would require labeling most digital media with a disclaimer because doing so would inure voters to these notices to the point that they would stop paying attention to them.
- **Warn About Deceptive Media, Not AI**: Mandatory disclosures should focus on alerting the public that the media in question is deceptive, not that it was produced using AI. For example, California's law requires a disclosure stating "This [image/audio/video] has been manipulated."[2] Such a disclosure is more informative for voters than stating "This [image/audio/video] was created with AI" and avoids creating a negative connotation around the use of AI.
- **Promote Robust Enforcement**: Transparency requirements for deepfakes will be useless if they are not accompanied by effective enforcement mechanisms. Otherwise, a campaign could spread deepfakes about their opponent a few days before an election knowing that no oversight and consequences would occur until after people have voted. Given the fast pace of elections, candidates should be permitted to seek injunctive relief against organizations distributing deepfakes about them, such as an order to stop running ads with deepfakes, as well as civil relief to compensate for harm and punitive damages as a deterrent.
- **Focus on Political Organizations**: State election laws should focus on setting rules for political organizations that create and share deepfakes, not on the intermediaries, such as email providers, streaming video providers, or social media networks, used by political organizations to share this content. States risk creating a multitude of overlapping and conflicting rules if every state creates its own laws dictating how online services should treat third-party political content potentially involving deceptive media.

AI IN STATE GOVERNMENT AGENCIES

The proposed legislation also outlines requirements for state agencies that use AI. Specifically, it would require Alaska's Department of Administration, at least every two years, to create an inventory of all systems state agencies use that employ AI for consequential decisions and conduct an impact assessment of these

systems. It would also impose certain obligations on state agencies that use AI for consequential decisions (i.e., decisions made by a government agency that have a significant or legal impact on an individual), such as notifying impacted individuals and obtaining consent before processing sensitive data. The legislation would prohibit using AI that involves data transfers to certain countries of concern, such as China and Russia. Finally, the legislation would impose civil liability on state agencies and state employees for harm resulting from reckless or negligent use of AI.

Creating clear rules for the use of AI in state government is important to ensure that agencies use the technology appropriately. For example, establishing guidelines can ensure that government agencies understand the limitations of these systems, address cybersecurity and privacy risks, and use the technology effectively, thus improving government productivity, better addressing their constituents' needs, and acting as good stewards of taxpayer dollars. Too often, government agencies fall behind in adoption technology, especially compared to the private sector.[3] Therefore, legislators should encourage government agencies to responsibly test and deploy new technologies like AI.

To ensure that rules do not restrict beneficial uses of AI in government agencies, policymakers should adhere to a few principles:

- **Treat All Automated Decisions Equally**: AI is not the only technology used to automate decision-making in government. For example, frontline workers may follow routine procedures or computer systems may impose certain fixed rules without any meaningful human oversight or discretion over consequential decisions impacting individuals. In all of these cases, individuals may suffer harm and face little recourse. Rather than creating specific oversight for decisions made, or augmented by, AI, policymakers should seek rules that broadly cover any automated decisions by government agencies.
- **Avoid Disincentives For Using AI**: Government agencies typically have limited resources, which means that workers often seek out the path of least resistance. When policymakers create hurdles that state agencies must jump through to use AI, they risk steering them towards non-AI solutions, even if those options are less optimal. Therefore, policymakers should ensure that any requirements they impose on government agencies that use AI are reasonable and proportional to the risks and that there are no unique obligations for AI systems that do not fall on similar non-AI systems. For example, data protection measures should generally apply to all systems that handle sensitive data, not just those involving the use of AI.
- **Facilitate Data Sharing**: Agencies need access to data to make use of AI. Increasingly, data spans multiple agencies, and therefore policymakers should work to reduce barriers to sharing data between agencies when done to advance the public interest or better serve their customers. At the same time, policymakers should ensure there is appropriate oversight to protect data, such as using deidentification methods and federated learning, and transparency, to ensure that individuals understand how agencies use their sensitive personal data.
- **Attract Top Tech Talent**: Government agencies are unable to make use of AI and other new technologies if they do not have workers with advanced skills. Sometimes government agencies struggle to attract top tech talent because the private sector may offer higher salaries. However, many technologists are attracted to the interesting problems government agencies work on, as well as the

opportunity to serve the public. But policymakers should be careful to avoid creating disincentives to working in government, such as imposing civil liability on technologists working in government that they would not face working in the private sector.

CONCLUSION

Advancements in AI are creating many opportunities to use the technology for beneficial purposes across virtually every sector, and people will undoubtedly find many useful applications for AI in elections and government agencies in the years ahead. As you consider legislation on this topic, please consider the principles outlined above to balance managing risk with enabling innovation. I look forward to working with you as you continue to refine this legislation.

REFERENCES

1. Steve Contorno and Donie O'Sullivan, "DeSantis campaign posts fake images of Trump hugging Fauci in social media video," CNN, June 8, 2023, https://www.cnn.com/2023/06/08/politics/desantis-campaign-video-fake-ai-image/index.html.
2. Cal. Election Code §20010.
3. Michael McLaughlin and Daniel Castro, "Benchmarking State Government Websites," August 27, 2018, Information Technology and Innovation Foundation, https://itif.org/publications/2018/08/27/benchmarking-state-government-websites/.