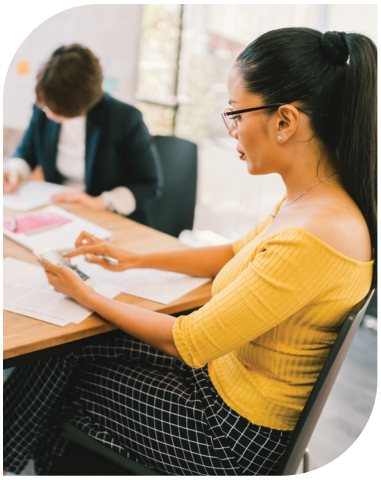

# TECH TABLE

## Digital Privacy and Inclusion

NCAPA believes that policy must evolve to consider ways to protect data and civil rights on the new digital frontier. The new technologies that are changing everyday life cannot be an equalizer of opportunity if people lack equal access.

## Open Internet

While consumer protections are crucial, NCAPA also believes that everyone should have equal access to the internet and digital platforms. It understands that the debate surrounding how to best regulate the internet is complex and welcomes debate; however, NCAPA also believes the following principles must be preserved: no blocking, throttling, or unreasonable discrimination.

## Recommendations

- **An individual's right to access must include their ability to request, update, change, dispute the accuracy of, or remove their personal information without penalty or discrimination.**
- **Companies must obtain opt-in consent prior to collecting or disclosing sensitive data such as genetic, biometric, or precise location data, or prior to disclosing data outside of the parameters of their relationships with a user.**
- **Personal information should only be disclosed to government entities after an appropriate judicial process.**
- **Consumers privacy laws should apply equally across the internet eco-system.**
- **Digital-based companies should allow users the ability to identify their preferred language for privacy notices.**
- **When a data breach occurs, the company should disclose the breach to its users in a timely manner, while also using plain language and offering translations. In the disclosure, the company should state how it plans to address the breach and when and how users should expect to receive updates about the process.**
- **Data practices should not discriminate against protected characteristics, including race, ethnicity, religious or political belief, gender identity, sex, income, language proficiency, or education level.**
- **Surveillance and data gathering tools and protocols should undergo regular audits to ensure responsible and equitable use.**
- **Private and public entities, including police departments and schools, must be regulated in their ability to use facial recognition technology and personal demographic data, especially in life-impacting decisions, such as employment, criminal justice, health, education, and money lending.**
- **Fund a diverse array of digital equity projects at the state and local level to help close the digital divide.**