

2025 STATE POLICY PRINCIPLES

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of American innovation by advocating a targeted policy agenda at the federal and 50-state levels. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents over 5 million employees and countless customers in the fields of information technology, artificial intelligence, e-commerce, the sharing and gig economies, advanced energy, transportation, cybersecurity, venture capital, telehealth, and finance. TechNet has offices in Austin, Boston, Chicago, Denver, Harrisburg, Olympia, Sacramento, Silicon Valley, Tallahassee, and Washington, D.C.

We encourage state leaders to adopt smart, adaptive, and long-range strategies that foster innovation, enhance global competitiveness, promote job growth and retention, build highly skilled workforces, create the energy and transportation systems of the future, invest in information technology, develop cyber awareness and digital literacy, and provide improved services to constituents with successful, consumer-oriented models.

The technology industry is a local, state, national, and international leader in job creation, product deployment, sustainable economic development, clean energy technology, and global competitiveness. TechNet's number one priority is to protect this economic engine and preserve the United States' leadership in innovation and productivity. In furtherance of this fundamental purpose, the TechNet state program will focus on eleven specific areas:

1. Privacy and Security
2. Artificial Intelligence
3. Education and Workforce Development
4. Energy and Environment
5. Financial Technology
6. Expanding Opportunity in the Innovation Economy
7. New Technologies and Future of Work
8. Autonomous Vehicles and Connected Vehicles
9. Procurement
10. Taxation
11. Smart Infrastructure

PRIVACY AND SECURITY

Consumers expect, and should expect, to trust the tech sector to protect their data. One of TechNet's top priorities is ensuring that governments focus on policies that harness market incentives to drive effective risk management and do not exacerbate harms to victims of criminal hacks.

Priority Issues

Privacy

Many policymakers and interest groups introduce and sponsor legislation targeted at data privacy and an individual's rights with respect to their personally identifiable information. Our member companies consistently place a high priority on consumer privacy, and the technology industry is committed to privacy and security. As part of that, transparency and the responsible use of data are pillars of the tech sector. TechNet will advocate for a federal privacy standard that expressly preempts state laws and brings uniformity to all Americans regardless of where they live, encourages innovation, and ensures that consumers' privacy is protected consistent with reasonable expectations and industry standards.

In the absence of a federal standard, lawmakers should look to interoperable, comprehensive legislation already passed in other states to build on the unified standard that already provides strong privacy protections to more than 100 million Americans. The state program supports the following principles:

- Any consumer privacy bill should be designed to build consumers' trust and foster innovation and competitiveness.
- Consumer consent, where applicable, should generally be required only for processing sensitive personal information and the data of known children or when there are material adverse changes to the processing of personal information previously collected. Consumers should have the right to opt out of the sale of their personal data and its use for targeted advertising. Any consent regime should be designed with the limitations of software, hardware, and data management in mind and should not be overly burdensome to the consumer or technology provider. It should also be flexible and convenient for all users regardless of socioeconomic or disability status.
- New privacy laws should provide strong safeguards to consumers while also allowing the industry to continue to innovate. New laws should be based upon an interoperable, uniform set of standards to avoid imposing a patchwork of policies across jurisdictions.
- Privacy laws should promote transparency about the use of consumer data and provide consumers with rights to protect personal data over which they reasonably seek to maintain privacy.
- Specific requirements related to data processing, including collection, use, disclosure, security, or retention, should be commensurate with the sensitivity of the data.
- Enforcement by a state's attorney general is the appropriate mechanism, and private rights of action and other tools that encourage litigation and lead to inconsistent enforcement must be avoided. A right to cure should be provided, and monetary judgments should be tied to actual harms caused by violations.
- Outright bans, prohibitions, or moratoriums on specific technologies should be avoided. Privacy laws should be technology neutral.
- State privacy laws should not apply to information already regulated by existing federal privacy laws or restrict access to publicly available information.
- Privacy laws should not limit consumer access to free, ad-supported services.
- Legislation should not force data controllers to share consumer data with third parties.
- Privacy laws should not treat data transfers across commonly owned affiliates as third-party transfers.
- Protecting everyone's privacy will protect children's, biometric, and health privacy. Lawmakers should prioritize comprehensive data privacy solutions based on a uniform set of standards that include rights for consumers of all ages, including the rights to access, correct, and delete personal data. Any legislation regarding children's, biometric, or health privacy should avoid conflicts with comprehensive data privacy laws.
- TechNet members routinely assess their online services and products for their compliance with existing privacy laws and their potential impacts on users, including child users. Legislation to account for the safety and privacy of child users should use a risk-based approach and provide clear, actionable guidelines to companies that develop online services and products for child users in order to ensure compliance.
- Lawmakers should align any state laws with the federal *Children's Online Privacy Protection Act (COPPA)* by, for example, defining "child" as "individual under the age of 13," including an actual knowledge standard, and focusing on online services "directed to children."
- Stringent age verification to access online platforms requires the collection, processing, and storage of users' sensitive personally identifiable information, like birth dates and government identification, and should be avoided. This conflicts with data privacy best practices like privacy by design and data minimization, creates new vectors for fraud, and eliminates anonymity online.
- Privacy laws should not broadly prohibit government use of third-party data, which is often an integral component of providing effective and efficient government services as well as protecting against fraud.

Cybersecurity

Cybersecurity continues to be one of the most significant challenges facing public and private entities in the modern digital economy. The technology industry invests significant resources to protect public safety, guard our operations from interruption and intrusion, and prevent the loss of capital and intellectual property. Due to

the nature of state statutes and local ordinances, legislation and regulation addressing cybersecurity issues can lead to the misallocation of limited resources through mandates that are overly prescriptive or technology-specific. These actions can hamper innovation and make impacted information systems easier targets for cyber criminals. Instead, we must protect and promote the ability of the private sector to be fast and agile in detection, prevention, mitigation, and response to ever-changing threats.

The state program supports the following principles:

- The internet is global and requires laws, policies, and regulations to reflect the global nature of the market.
- State and local governments should set positive examples for private sector businesses by effectively managing the security of their own networks through application of risk-based frameworks, dedicating necessary resources to manage critical IT systems, and focusing investment on modern technologies capable of being effectively secured. Governments should prioritize identifying technology at the end of its lifecycle, ensuring a proactive approach to managing cybersecurity risks.
- Cohesive and adaptable national guidelines for security based on widely accepted industry best practices are preferable to varying state or local mandates to provide consistent, clear standards for companies to follow. State efforts to create cybersecurity regulations threaten federal harmonization efforts and force businesses to divert resources from security to compliance. Private and public sector organizations widely embrace NIST's Cybersecurity Framework (CSF) as a risk-based tool for prioritizing cybersecurity investments. Policies aimed at establishing best practices should be grounded in the CSF.
- Policymakers should encourage good cyber hygiene, modern technology, leading industry practices, and high-skilled cyber workers. Specifically, market-based incentives or safe harbors should be used to encourage companies to actively manage risks in accordance with widely accepted industry standards and best practices.
- Encryption and tokenization are fundamental technologies necessary to protect the security of critical systems and sensitive information. Governments should not demand changes that require backdoors, weaken encryption, or erode other reasonable security measures.
- A comprehensive, risk-based cybersecurity strategy should increase the security and resilience of all networks and end-user devices and prepare for and mitigate cyberattacks through the coordination of industry and government.
- Cybersecurity policies should focus on enhancing the confidentiality, integrity, and availability of information networks and end-user devices utilizing national and internationally recognized standards and data and provide for legal safe harbors to incentivize government and businesses to take steps to ensure that there are policies and procedures in place to protect against network intrusions.
- Security is an ongoing process aimed at managing risks that requires sustained and ongoing investments in people, processes, and technology.
- Securing internet-connected devices requires flexible security features appropriate to the nature and function of the device to prevent unauthorized remote access.
- Governments should maintain industry-leading cybersecurity practices and not require businesses to share data that it cannot keep safe and secure from threats.
- Reporting cyberthreat intelligence information to the government should be voluntary and include protections that ensure reported information is exempt from Freedom of Information Act requests, cannot be used as the basis for regulatory or enforcement actions, retains all legal privileges, and may not be introduced as evidence in any court proceeding. In addition, governments should reciprocate by sharing relevant cyberthreat information with the private sector to enhance the collective capacity to prevent and mitigate cybersecurity risks.
- Cybersecurity incident reporting should be compatible with existing federal laws and only require reporting once a covered entity is reasonably certain that a covered incident has occurred. Requirements linked to suspected or threatened incidents will result in excessive costs for businesses and governments without yielding actionable information. Additionally, reporting requirements should not include requirements to share trade secrets or intellectual property, as that will increase risk for companies.

Data Breach

Data breach policy focuses on the responsibility and requirements following what is almost always a malicious

attack on a public or private entity that has successfully accessed or otherwise compromised consumer and proprietary business data. Public policy in this area should be risk-based and focused on the likelihood of actual harm to consumers.

The state program supports the following principles:

- A single, national standard focused on protecting people from substantial harm is preferred because it would provide companies and customers with consistent, actionable notice of a data breach.
- Notice requirements that are not related to actual harm only burden companies and confuse customers with notifications that are not actionable. These requirements should be uniform across agencies and jurisdictions, maintain consistent thresholds for reporting, and provide a reasonable notice timeframe.
- The distinction between an account takeover and a data breach should be explicitly recognized in data breach statutes, with differentiated provisions and reporting methodologies.
- Data rendered unusable by encryption, redaction, or any other security method or technology should be considered out of the scope of data breach reporting requirements because the risks of harm are not cognizable.
- Data breach notification policy should only impact an entity if their network or system has been breached and acquisition of personally identifiable information has occurred. Reporting requirements that relate to unsuccessful attempts are not risk-based, will waste limited resources, and result in cumbersome contractual terms that create friction without providing any substantive benefits to data subjects. Entities should not be held responsible for, or be required to rectify, breaches outside of their control or responsibility.
- The statutory definition of personally identifiable information should be limited to only a subset of “personal information” covered by applicable data privacy laws. That subset should be personally identifiable information that, if compromised, could lead to identity theft or other substantial harm.
- Public safety entities should be provided the appropriate level of resources to help deter, identify, track, and punish this criminal behavior.
- Private rights of action, civil penalties, and other tools to encourage litigation will reduce the effectiveness of a data breach notification standard by discouraging reporting without providing substantive breach protections.
- Policymakers should encourage privacy by design, good cyber hygiene, modern technology, leading industry practices, and high-skilled cyber workers. Specifically, market-based incentives or safe harbors should be used to encourage companies to actively manage risks in accordance with widely accepted industry standards and best practices.
- Companies should have adequate time for internal or external investigations, including by law enforcement, to determine the nature of an incident and whether it constitutes a data breach.
- Any requirements that vendors notify state IT agencies should follow existing law regarding breach notifications or the time period specified in the applicable terms of the contract between the state agency contractor and the state agency.
- Obligations to report data breaches and security incidents to state authorities should be limited to one agency per state, ideally the state’s attorney general. Obligations to provide duplicative reporting to multiple state agencies create an undue burden on businesses as they are actively responding to an incident.

Secure and Safe Repair

Consumers, small and large businesses, public schools, hospitals, banks, and manufacturers all need reasonable assurance that those they trust to repair their connected products will do so safely, securely, and correctly. Proposals that require original equipment manufacturers (OEMs) to provide unaffiliated repair firms with access to proprietary schematics and repair, diagnostic, and security tools create major risks to consumer safety and privacy and the security of connected infrastructure.

The state program supports the following principles:

- OEMs and authorized repair firms are uniquely qualified to ensure the secure and safe repair of electronic products. These firms use OEM-trained technicians and original parts that are backed by the

OEMs and their partners with warranties, legally enforceable contracts, quality assurance requirements, and other mechanisms that provide strong protections for consumers.

- Requiring manufacturers to disclose diagnostic tools, source code, and software developed by the manufacturer at significant cost and provide access to tightly controlled supply chains to unaffiliated, unvetted third parties would place proprietary corporate information and sensitive customer information in the hands of unknown actors, creating a new set of intellectual property rights concerns and cybersecurity vulnerabilities.
- Private rights of action and other tools to encourage litigation must be avoided.
- Legislation should avoid a patchwork of inconsistent policies that will stifle innovation and/or are technically or operationally infeasible.

Facial Recognition and Biometric Technology

Facial recognition technology and other forms of biometric identification can be utilized in a variety of use cases, many of which can improve security and access for individuals using services. Biometric technology can enable remote access to essential services, removing location- and mobility-based barriers to access. In addition, different types of biometric technology can be used to facilitate entry, stop fraud, and protect consumers.

The state program supports the following principles:

- TechNet will oppose any legislation that prohibits or effectively prohibits the use of facial recognition or biometric technology except where there is a specific, unacceptably high-risk case identified and the legislation is narrowly tailored to address that unacceptable risk.
- Legislation regulating the use of biometric technology should not provide for private rights of action, and any damage awards should be limited to instances where cognizable forms of actual economic harm have been demonstrated.
- Legislation should not reduce access to non-identifiable diverse datasets necessary to train models to reduce bias.
- Policies should recognize the wide variety of use cases for technologies that detect and/or recognize faces or other parts of the human form, and policies should avoid over-regulating visual technologies that do not affect individual privacy.
- Cohesive and adaptable national guidance is preferable to individual state mandates to provide consistent, clear standards for companies to follow.

Government Requests for Data

Governments occasionally request data regarding consumers from data controllers. Consumers' privacy should not be restricted except in narrowly defined circumstances based on clearly defined laws and standards, and any restrictions should be necessary and proportionate for the relevant purpose.

The state program supports the following principles:

- Disclosure of data should require proper authority and a valid legal process to be served and be consistent with the federal *Stored Communications Act* and the Data Privacy Framework under Executive Order 14086.
- Unless infeasible, a government should seek information from the entity contracting for cloud-based technology services instead of from the third-party providers who are not party to or the subject of a governmental investigation.
- Where valid legal process is not required, government requirements for the disclosure of consumer data should be for deidentified and aggregated data.
- Companies have the right to push back on overly broad or vague requests and seek attestation about the cause for a request for disclosure.
- Disclosure requirements should not contain arbitrary or unreasonable timelines for disclosure.
- Requirements for company disclosure of data under a non-disclosure order should contain a reasonably and clearly defined expiration date for that order.

- In cases where state-level data privacy laws are already in place, local rulemaking must align with state standards on consumer data protection, restricting the extent to which local authorities can mandate data disclosures.

Content Moderation

Online services enable freedom of expression for consumers, and companies have a vested interest and a First Amendment right to moderate their platforms to create a safe, welcoming online community for users. To ensure that online services are inclusive, useful, and safe for consumers, online platforms often moderate the content posted by users. In order to ensure users understand the rules they are expected to follow, the industry has been at the leading edge of providing greater access and information regarding their moderation policies and practices.

The state program supports the following principles:

- Governments should not restrict or penalize online platforms' efforts to exercise their First Amendment rights to moderate content on their private platforms.
- Governments must recognize companies' rights to enforce their terms of service and respond to evolving threats.
- Governments should avoid mandates that require companies to affirmatively search for and report content on their platforms. Such mandates have the potential to transform private platforms into agents of government and thereby create complex constitutional challenges for both platforms and law enforcement.
- TechNet supports clear, constitutional definitions that are consistent across jurisdictions.
- TechNet supports industry efforts to provide transparency about platforms' content moderation practices and their efforts to limit and remove harmful content. These policies should not mandate or prioritize the policing of certain categories of content and should not undermine platforms' efforts to moderate harmful content, including by requiring disclosure of otherwise confidential information.
- TechNet supports industry efforts to provide users with greater control over their online experience, including tools that allow users to better curate the content they see and the features they use based on their preferences. States should avoid policies that mandate or prohibit certain features or tools and instead focus on incentivizing platforms to provide users an increased ability to manage their experience on the platform.

Children and Teens' Digital Well-Being

TechNet's member companies prioritize the safety and well-being of children who access their sites and platforms. Our members strongly believe children deserve a heightened level of protection, and TechNet members have been at the forefront of raising the standard for digital well-being across the industry by creating new features such as settings, parental tools, and protections that are age-appropriate, empower families to create the online experience that fits their needs, and are tailored to the differing developmental needs of young people.

The state program supports the following principles:

- State laws should respect and uphold the First Amendment and avoid burdening lawful speech. State laws should not conflict with any relevant federal law.
- States should not implement laws that broadly restrict access to online services for all users under the age of 18. Instead, any law seeking to restrict access to online services should consider the various nuanced ways in which older teens utilize the internet differently from children and the benefits or potential harms of those uses. It should be narrowly tailored to the appropriate age groups at issue and alleged specific harms. States should also take care not to restrict advertising too broadly, which can have the effect of restricting access to otherwise free services or relevant information for participation in civic life.
- States play the lead role in K-12 education policy, including what students should learn and when. State lawmakers should encourage the adoption of instructional standards regarding digital and media literacy, as well as internet safety for use at multiple grade levels.

- School districts, with the guidance of parents, are best positioned to establish standards for how school-issued devices can be used by students to ensure all students have access to the technological tools essential in today's modern economy and schools.
- Online platforms have created numerous digital tools to help parents control their children's digital experiences. Lawmakers should seek opportunities to amplify these resources and educate parents on how they can be utilized, as parents know what is in the best interests of their child.
- Lawmakers should focus on the harms they wish companies to mitigate, rather than trying to dictate specific features or design choices. Any prohibited activities or harms should be stated with specificity so the companies know precisely what to prevent, and any knowledge standards for liability should be set at "knowing" and "intentional" so that bad actors are the focus of the law, not bad definitions.
- Regulation should enable parents to protect their children online without overstepping the duties of a parent. It should acknowledge the primary role that parents have in ensuring their children's safety online and focus on addressing the underlying challenges that parents face to ensure their safety.
- Enforcement by a state's attorney general is the appropriate mechanism, and private rights of action and other tools to encourage litigation must be avoided. Litigation leads to uneven and inconsistent policy outcomes, with companies choosing to limit their legal exposure differently. A single regulator, the opportunity to seek and receive guidance, and the opportunity to correct good faith mistakes will ensure greater compliance with the law and more consistent protections for child users.

Learn what TechNet member companies are doing to keep kids safe on their platforms [here](#).

ARTIFICIAL INTELLIGENCE

Artificial intelligence (AI), machine learning (ML), and the algorithms that often support artificial intelligence have generated policymaker interest. We acknowledge that as technological advances emerge, policymakers' understanding of how these technologies work is vital for responsible policymaking. Our member companies are committed to responsible AI development and use. TechNet will advocate for a federal AI framework that brings uniformity to all Americans regardless of where they live, encourages innovation, and ensures that consumers are protected. TechNet therefore supports the following principles:

- Comprehensive, interoperable data privacy laws should precede AI regulations.
- Avoid blanket prohibitions on artificial intelligence, machine learning, or other forms of automated decision-making. Reserve any restrictions only for specific, identified use-cases that present a clearly demonstrated risk of unacceptable harm to a user or a clearly articulated and demonstrable national security threat, and narrowly tailor those requirements to the harms identified.
- Encourage the creation of AI task forces with robust industry participation, which establish a line of communication, provide industry expertise on AI, and allow for the development of consensus frameworks on reasonable AI regulations. Ensure small businesses have opportunities to participate on AI task forces to ensure SMBs can access the benefits of AI technology.
- Ensure any requirements are clearly allocated to specific roles in the artificial intelligence value chain. Recognize the different roles and responsibilities of participants within the AI value chain, including their technical limitations, and regulate them distinctly as appropriate.
- Do not force participants within the AI value chain to share publicly information that is proprietary or protected, and do not require an AI registry.
- Avoid new policies or regulations that are duplicative or conflict with existing laws and regulations.
- Leverage existing authorities under state law that already provide substantive legal, anti-discrimination, and civil rights protections, and limit new authorities specific to the operation of artificial intelligence, machine learning, and similar technologies where existing authorities are demonstrably inadequate. Allow measures taken to comply with one law or regulation to satisfy the requirements from another applicable law or regulation if such measures and requirements are reasonably similar in scope and effect.
- Ensure any requirements on automated decision tools focus on high-risk uses where decisions are based solely on automated decisions. Avoid labeling entire sectors as inherently high risk, and focus on

- specific outcomes that involve the loss of life or liberty or have significant legal effects on people.
- Do not impose opt-out requirements that conflict with practical realities or functionality that serves consumers' interests.
- Regulation should encourage clear disclosure of AI systems where a reasonable person might otherwise believe they are interacting with another person — e.g., use of simulated personas like chatbots should be clearly identified.
- Offer technically correct, feasible, and nuanced definitions for key terms and roles within the AI value chain, in accordance with existing state and federal legislation and emerging industry standards. Policymakers should avoid overly broad definitions, such as those that use "including but not limited to," and instead adopt context-specific definitions that accurately address the diverse characteristics of AI applications, ensuring clarity on what is affected without encompassing common technologies or processes.
- Limit enforcement to relevant state agencies and avoid private rights of action. Ensure any enforcement actions limit damage awards to clearly cognizable forms of actual demonstrated harms directly resulting from violations of the law. To promote balanced enforcement, legislation should include a right to cure, rebuttable presumptions, and allow for affirmative defenses, giving businesses a reasonable opportunity to correct potential violations.
- Provide safe harbors for companies that test and mitigate any bias or issues found in AI systems, as well as a reasonable right to cure period upon notice.
- Ensure data, including sensitive data with sufficient cybersecurity and privacy protections, can be used to conduct internal testing and model training to ensure algorithms work inclusively and as intended.
- Avoid a one-size-fits-all policy approach and support a risk-based framework that ensures that comparable AI use cases are subject to consistent oversight and regulation across sectors.
- Rely on self-certification mechanisms wherever possible, and avoid mandating external or third-party audits of impact assessments or risk assessments. Rather, identify the audit or assessment requirements and goals, allowing companies to determine if they are capable of conducting the audit or must seek third-party support.
- Rely on established national and international standards and frameworks, including the NIST AI Risk Management Framework and ISO standards, to guide policy discussions to ensure interoperability and avoid a patchwork of inconsistent regulations.
- Avoid holding developers, deployers, or distributors of AI and automated decisionmaking technologies liable for any unknown or unforeseen circumstances that may arise from the use and deployment of their technologies.
- Ensure any requirements on content provenance allow for flexibility of provenance techniques across various modalities (image, audio, video) and take into account the risk of the model for misuse.

Deepfakes

- Legislation should protect against intermediary liability when regulating the creation and use of deepfakes.
- Any disclosure or disclaimer requirements for electoral materials containing a deepfake should be placed on the candidate or sponsor of the material.
- Legislation should not disrupt the use of innovative technologies to detect deepfakes in order to protect against cybersecurity attacks and fraudulent activities.
- TechNet members are active in developing protections against the creation, storage, and distribution of child sexual abuse materials (CSAM) already, and members collaborate with one another to better fight CSAM. CSAM is contraband in all contexts, and states should ensure that criminal liability is placed squarely on the criminal actors who create and disseminate such material. The actions taken by companies, including collaboration with law enforcement, to prevent, detect, protect against, report, or respond to the production, generation, incorporation, or synthesization of such material should be protected.

EDUCATION AND WORKFORCE DEVELOPMENT

With global economic leadership at stake, education and workforce development are more critical than ever. TechNet supports policies that help prepare our students to be a successful part of a global, interconnected, and technology-driven economy. The state program supports the following principles:

- Full funding for our public schools in order to give school leaders the resources and flexibility needed to innovate and deliver the highest quality education to all students in K-12, higher education, and beyond.
- Digital learning resources and technology integration in student learning environments to improve student outcomes and enable college and career readiness.
- The recruitment and training of qualified teachers and innovative school administrators.
- Increased access for students to high-level STEM, computer science, information technology (IT), operational technology, and coding courses, with a focus on underrepresented students including women, people of color, and individuals with disabilities.
- High standards and accountability.
- Workforce and skills development programs that are aligned with the needs of students, workers, and businesses and recognize the value of continuous learning as well as alternative educational pathways toward digitally resilient jobs.

Drive Innovation in the Classroom

- Digital learning: Promote the use of digital content and tools to provide individualized, data-driven learning and improve educational outcomes.
- Champion hands-on, project-based learning to drive collaboration, creativity, communication, and critical thinking skills.
- Consistent, strategic funding: Support efforts to secure stable funding for digital education, aligned with a statewide vision to expand and promote digital innovation inside and outside of the classroom.
- Infrastructure: Support measures that focus finances, partnerships, and strategies to close the digital divide in urban and rural communities in order to ensure that all schools have sufficient infrastructure and secure network connectivity with the necessary speed, capacity, flexibility of choice, and reliability to support “smart” classrooms and provide sustained IT support to maintain and upgrade systems.
- Innovative technologies: Ensure students and instructors have access to transformative technologies as well as the training and education necessary to use those technologies to remain competitive with the skills of tomorrow.

Recruit and Develop Qualified Teachers and Innovative Administrators

- Professional development: Support dedicated funding for sustained and robust training for high-quality STEM and computer science teachers, both pre-service and in-service.
- STEM teacher shortage: Support efforts that address the severe shortage of qualified STEM, computer science, and IT teachers and develop a sustainable pipeline of talent.
- Teacher certification: Support the establishment of computer science and IT certification pathways that ensure all computer science and IT teachers have appropriate knowledge of and are prepared to teach the curriculum.
- Empower teachers and administrators: Support programs that empower teachers and administrators to make informed decisions on the procurement of technology, leverage technology to evolve classroom teaching and administration, and improve collaboration through communities of support.

Expand Access and Inspire Students

- Underrepresented students: Support policies and programs that focus on engaging and providing opportunities for low-income students, women, people of color, and people with disabilities in STEM

subjects, computer science, and IT. Support public and private partnerships committed to developing both a diverse workforce pipeline and opportunities for job placement.

- Early and broad exposure: Support policies and programs that ensure principles of computer science, IT, computational thinking, communication, and STEM skills are integrated, where possible, in other subjects of K-12 instruction.
- Awareness and inspiration: Support school and public/private programs that inspire the next generation of students to pursue STEM and computer science and IT careers and educate parents about opportunities in these fields.

Prepare for Digital Risks in Classrooms and Schools

Students and educators deserve to learn and work in an environment that is safe and secure physically and digitally. With this in mind, we support the following principles:

- Ongoing K-12 cybersecurity risk management: Adopt a proactive approach to addressing cybersecurity risks.
- Prioritizing and implementing mitigation strategies for K-12 systems: Identify the most critical risks and apply mitigation strategies such as multi-factor authentication, robust password policies, phishing prevention, software updates, and related professional development and upskilling for school personnel.
- Planning, budgeting, and forecasting for cybersecurity incidents: Develop and practice cybersecurity incident response plans to minimize the impact and prepare for potential cybersecurity breaches.
- Productive learning environments: Support initiatives to create productive learning environments, provided any efforts continue to support digital learning resources and technology integration.

Promote High Standards and Accountability

- Make computer science count: Ensure that a qualified computer science course may fulfill a core science or math high school graduation requirement.
- Implement rigorous computer science standards: Ensure computer science standards are focused on computational thinking skills and the creation and ethical use of software and other computing technologies.
- Use data to drive accountability and measurable learning outcomes: Support rigorous standards for students and the transition to data-driven assessments that provide a clearer picture of what and how students are learning and if they are developing the skills necessary to be college-ready and successful in the global marketplace. Support the use of data to enhance personalized learning, improve assessment and feedback, optimize resource allocation, and foster early intervention.

Classroom to Career/Skills Development

- Align the resources of educational and training systems with the needs of technology industry employers: Promote programs that award industry-recognized certifications to validate skills and job-readiness, as well as programs that include partnerships with industry.
- Support high-quality career and technical education (CTE): Ensure CTE programs advance academic, technical, and industry-relevant technology skills and collaboration and communication skills to prepare all students for success in college and technology-rich careers. Improve the link between education and employment so learners are prepared for in-demand jobs.
- Increase access, affordability, and completion of postsecondary education and bridge the divide between higher education classroom learning and work: Expand access to real-world applied learning opportunities like internships and apprenticeships.
- Promote lifelong learning, retraining, and reskilling policies and programs that allow workers, including independent workers, to attain the education and skills they need to stay current and advance their careers as jobs evolve.
- Streamline the eligibility process for accessing training funds, which could further leverage investment from the private sector through employer-directed training.
- Improve access to and promote traditional and nontraditional pathways to employment to help more job seekers across all demographics access in-demand, skills-related education and training programs.

- Promote skills-based hiring practices in order to expand the talent pool for employers and remove barriers for workers, including the removal of unnecessary degree requirements for employment.

ENERGY AND ENVIRONMENT

TechNet supports policies that are technology-neutral and that foster and promote innovation in clean energy supply and demand for a sustainable climate. This allows companies to create, thrive, and compete in the United States and around the globe. Technology is a significant driver of efficiencies and innovative solutions for solving a wide range of environmental issues, so it should be fostered through smart policy and research and development funding. TechNet's state program supports the following principles:

- A robust, technology-neutral energy agenda that will spur the development and deployment of clean energy and clean transportation resources and technologies.
- Customer choice.
- Resilience and reliability in the face of security threats, natural disasters, and uninterrupted energy supplies. Understanding that clean energy and resilient energy are not mutually exclusive, TechNet will seek to advance the intersection of sustainable energy and resilient energy.
- The expansion of competitive and transparent energy supply markets at the wholesale and retail levels.
- Forward-looking policies that ensure open access and enable market-based deployment of wholesale and distributed energy resources.
- States should support deploying new transmission lines and upgrading existing transmission lines to expand and fortify grid infrastructures with grid-enhancing technologies (GETs), reconductoring, and other innovative solutions that reduce congestion and transmission constraints.
- Fair and equal access to data, in a standardized format, to enable industry growth while empowering consumers to effectively deploy and utilize clean energy and clean transportation solutions.
- Stable tax policies that provide industry and consumers with long-term clarity to support the investment in and deployment of clean energy technologies.
- Policies that recognize the contributions of companies with voluntary clean energy initiatives that move faster than state goals, such as accelerated renewable energy buyer provisions in Clean Energy Standards and Renewable Portfolio Standards.
- Policies that provide support for green jobs, including training and upskilling.

Environmental Stewardship

TechNet member companies have developed and continue to maintain significant policies and practices that protect the environment, address climate change, and promote sustainable conservation, recycling, and waste reduction. Technology is used to drive efficiencies, reduce waste and emissions, and create innovative solutions for environmental challenges. Efforts to expand or create new mandated environmental programs should be inclusive, balanced, flexible, and data-driven in order to achieve stated aims and avoid significant disruption.

Environmental Applications of AI

Artificial intelligence can assist with tackling the world's greatest environmental challenges. To promote these efforts, governments should create and maintain open-source environmental data and forecast databases, making them freely accessible to train AI models. Working together, industry and governments can leverage these climate models and forecasts to turn big data into actionable information and accelerate the research and development process.

TechNet will support policies that foster collaboration between government, private sector, and academia to accelerate environmental applications of AI, including the option to open source these learnings and best practices to ensure the benefits of AI are shared with communities that may lack the resources to implement such technologies independently.

TechNet will support policies to leverage grants and tax incentives to promote the environmental applications of

AI, which can unlock new opportunities. For example, AI can help to optimize critical systems like the electricity grid or detect and monitor wildfires and illegal deforestation.

Energy Appendix

TechNet's clean energy priorities include advocacy and support around the following policy areas; further details on each of these can be found in the Appendix.

- Demand Response (DR)
- Distributed Energy Resources (DER)
- Energy Efficiency Standards
- Resilient Energy Supply
- Clean Energy Standards, Renewable Portfolio Standards, Alternative Portfolio Standards, Renewable Fuel Standards, and Low Carbon Fuel Standards
- Grid Modernization
- Retail Energy Competition and Self-Supply
- Grid and Customer Data Access and Transparency
- Electrification of Transportation
- Clean Energy Supply
- Microgrids
- Demand Charges

FINANCIAL TECHNOLOGY (FINTECH)

TechNet promotes the banking and financial technology (fintech) sectors by removing regulatory barriers to financial access and literacy, economic growth, and job creation. TechNet supports innovation in the banking and fintech sectors by encouraging state policymakers to ensure the regulatory system remains technology-neutral and regulates new technologies, including digital currencies and alternative banking, using a balanced approach that encourages fair competition and promotes access to competitive financial services.

TechNet supports private sector efforts to provide consumers with new, safe, secure, reliable, and accessible financial tools. In particular, the state program supports the following principles:

Financing Reforms

- Policymakers should prioritize updating antiquated state regulations to remove barriers to an integrated, digital transaction by addressing the role of technology in enabling constant change, diversity, and innovation in financing.
- Policymakers should encourage and advance financing laws and regulations across jurisdictions that account for and preserve access to the innovative lending market of today, oppose adding fees or additional requirements to global transactions, and authorize the use of digital tools such as e-signatures, remote online notarization, and automated valuation models to promote efficient, streamlined financial transactions.
- Policymakers should promote industry best practices that protect consumers and small businesses, such as transparent disclosures, without inhibiting innovation in providing access to credit.

Financial Empowerment

- Leverage technology to reduce barriers to financial literacy and services and empower consumers and small businesses to better manage their financial lives.
- Unlock the power of financial apps. Policymakers should empower consumers and small businesses to take advantage of financial apps on their smartphones that improve security and offer reliable convenience and give unbanked and underbanked persons opportunity to build credit.

- Unlock access and promote education and training of digital tools that improve financial literacy for all consumers and small businesses.

Payment Systems

- Enhanced security and convenience through continuous innovation. No one technology should be mandated for security and authentication, nor should one technology become a *de facto* mandate through “floor-setting.”
- Promote new entrants and empower consumers and small businesses to utilize a broad array of fintech products and solutions.
- Promote the adoption of and oppose restrictions on card and mobile retail.
- Reduce fraud in the financial industry by empowering innovators.
- Promote free market growth of the payments industry to provide consumers and small businesses with secure and efficient payment options, and defend it against market-controlling legislative and regulatory policies.

Digital Assets, Blockchain Technology, and Web3

- Encourage policymakers to take a measured approach toward digital assets, blockchain technology, and Web3 through legislative proposals that conduct studies of these emerging technologies amongst key state regulators where policymakers can first develop a fact basis for understanding the costs and benefits of emerging technologies and only seek to regulate to fill gaps in existing law.
- Encourage states to adopt the Conference of State Bank Supervisors’ *Money Transmission Modernization Act* (MTMA), a model law drafted with the goal of creating a single set of modernized nationwide standards and requirements.
- Identify the benefits that would accrue to state governmental operations by incorporating digital assets, blockchain technology, and other emerging technologies into how citizens interact with state government.
- Promote cooperation across state securities regulators, other state financial regulators, and state attorneys general to prevent a patchwork of inconsistent state regulations that could stifle innovation.

EXPANDING OPPORTUNITY IN THE INNOVATION ECONOMY

The technology industry is committed to promoting an inclusive workforce that reflects the diversity of our country and our customers. We support education, workforce development, and immigration policies that empower all people to continue making important contributions to our nation and communities.

In the majority of states, there are no clear state laws banning discrimination based on sexual orientation or gender identity. In recent years, there have been hundreds of bills and ballot initiatives proposed that would eliminate non-discrimination protections or that explicitly authorize discrimination by individuals, businesses, and state and local agencies.

We oppose any legislation, by any name, that would legalize discrimination on any basis, including nationality, race, religion, age, disability, natural hair texture, sexual orientation, and gender identity, and that would therefore impact workforce recruitment efforts, complicate human resources administration, and undermine the technology community’s commitment to diversity and inclusion. We recognize the opportunity for and responsibility of the technology industry to lead in the creation and implementation of more inclusive policies nationwide.

Diversity, equity, and inclusion (DEI) policies are essential to corporate missions as we seek talented individuals diverse in age, race, gender, geography, and points of view to work in an environment where employees are valued and have opportunities to contribute, advance, and succeed. Policy proposals should not restrict corporate programs or intervene with prescriptive requirements or liability.

We recognize the valuable contributions immigrants make to our economy and country as a whole. For example, immigrant entrepreneurs have started more than half (319 of 582) of America's startup companies valued at \$1 billion or more. We oppose state policies that unfairly target immigrant communities and support action at the federal level to reform our high-skilled immigration system to curb abuses and ensure that more green cards and visas are available to help fuel innovation at our research institutions and universities and address the high-skilled labor shortage facing the U.S. economy. We also support a permanent federal legislative solution for Deferred Action for Childhood Arrivals recipients, or "Dreamers."

As millions of Americans express deep frustration over long-simmering racial disparities, we urge policymakers to listen to communities of color and develop proposals that will help to remove institutional barriers to opportunity and reverse racial inequities in our society. TechNet supports efforts to combat systemic racism, including investing in underrepresented communities to close entrepreneurship and wealth opportunity gaps, supporting reforms to reduce racial inequalities in the criminal justice system, and promoting efforts to close the gaps in racial disparities in education.

NEW TECHNOLOGIES AND FUTURE OF WORK

State legislatures, local jurisdictions, and courts across the country have reacted in different manners to the rise of new technologies-and increased opportunities for people to provide goods and services. Policies will fail to serve constituents if they are not informed by the companies that are expected to implement them, are overly sweeping, or rooted in misperceptions. Any new legal or regulatory requirements should be tailored to the product and associated industry, directly tied to an identified harm, limited to gaps in existing coverage, focused on bad actors, and narrowly tailored to avoid conflicts or discrepancies in the law and unintended consequences. One-size-fits-all approaches must be avoided given the variety of industries, different technology models, and varied reasons why people seek or provide services. In addition, corresponding rules and regulations that apply to legacy providers should be adjusted accordingly to allow for technological neutrality. TechNet promotes policies that encourage the development of entrepreneurship, mobile commerce, and the next wave of innovation in the economy. Establishing an innovation-friendly policy framework is the key to the competitiveness of the technology industry. The state program supports the following principles:

Reasonable Statutory and Regulatory Framework

New technologies bring new products and services to the market. Occasionally, these new products and services generate significant policymaker interest because of transformative features with little precedent and high consumer interface. Autonomous vehicles, peer-to-peer car sharing, unmanned aerial vehicles, blockchain, digital assets, and self-service healthcare, including telehealth, teledentistry, and digital-forward pharmacy, are examples.

While some lawmaking may be needed or helpful, TechNet will be vigilant against vague, overbroad, unnecessary, harmful, or hostile laws and regulations that stifle innovation. Generally speaking, TechNet is supportive of efforts to modernize legal frameworks that aim to sensibly regulate novel products and services if they:

- Seek to encourage, enable, and advance American leadership in innovation.
- Support the underlying and future innovation inherent in the product or service.
- Focus on prohibiting negligent, reckless, or criminal conduct and on the actors rather than the technology.
- Avoid duplicating existing requirements and creating unclear overlap or conflicts with existing requirements, particularly where there are uniform federal regulations.
- Encourage a deliberate exploration of regulatory and non-regulatory approaches with a preference towards non-regulatory approaches unless there are high-risk outcomes that warrant more direct government approaches.
- Support an expeditious regulatory process to align with the speed of developing technologies.

- Recognize the benefits of the new technology.
- Continue to provide safeguards against intermediary liability, including opposing the application of strict liability onto online marketplaces.
- Recognize the ability for internet platforms to keep their users safe online by moderating content without creating liability risks.

Patient Access to Health Care

Telehealth is fundamentally altering how patients experience care. New telecommunications technologies allow health care professionals to provide patients with medical care and services in convenient, affordable, and accessible ways and enable health care providers to deliver and coordinate health care safely and at a high quality.

TechNet supports the following principles:

- Statutes should affirmatively enable the use of technology to treat patients remotely and ensure that the clinician-patient relationship can be established using technology. Prescribing must also be allowed using technology. States may allow for the prescription of controlled substances using technology in line with federal standards.
- Telehealth statutes should be technology-neutral and enable innovation, including allowing the use of both synchronous and asynchronous technologies.
- The use of “store and forward,” text messaging, remote patient monitoring, and other SMS technology should be allowed as clinically appropriate.
- Photography used to assist in the practice of telehealth should not require professional licensure.
- A health care clinician may provide a professional second opinion to a patient as long as the clinician is licensed or registered and in good standing in their resident state, provided that the physician is not involved in the treatment of the patient in the state where he/she is not licensed.
- State should adopt licensure compacts to facilitate patient choice and access and streamline clinician licensing.

Uncrewed Aircraft Systems

Commercial drone operations are already providing essential services to the American public and the Federal Aviation Administration (FAA) is developing a regulatory framework to further unlock operations that will provide workforce, economic, and environmental benefits to the communities where they operate. TechNet supports the following principles:

- The Federal Aviation Administration has exclusive authority to regulate aviation safety and use of the airspace by aircraft in the United States. State-by-state airspace laws will create a web of complex and confusing regulations that jeopardize safety for all airspace users and place unnecessary burdens on companies engaging in a new industry and place unnecessary burdens on companies engaging in a new industry.
- There are existing state and local laws that establish privacy protections, prohibit voyeurism, and forbid nuisances that apply to drone operations. Drone-specific legislation to provide further protection is unnecessary and onerous.

Access to Markets

While policymakers must balance new innovations with consumer protection, TechNet opposes regulatory restrictions imposed to protect existing markets from competition, such as excessive insurance requirements, prohibitive licensing requirements, caps on the number of services provided, limitations on where services can be provided, and unreasonable barriers to market entry.

TechNet supports legislation to protect consumers when it is based on an identifiable harm that has occurred or could occur. TechNet opposes legislation that regulates specific technologies based on unknown impacts to a consumer. In circumstances where policymakers have identified a significant threat or occurrence of harm that is not already prohibited or otherwise addressed by existing law or regulation, the cost, difficulty, and

practicality of implementing new rules and regulations should be analyzed against the magnitude and probability of potential harm. Further, policymakers should note the difficulties inherent in state or local regulation of companies and products that are multi-state or global in operations, including the interplay of other state or federal legal requirements.

TechNet supports efforts to increase access to capital, including intrastate crowdsourcing and other cutting-edge funding mechanisms.

Service Fee Regulations

TechNet opposes regulations that aim to cap or otherwise control technology companies' ability to price their own goods and services in line with their business models and consistent with freedom of contract principles. Technology companies' fees enable them to facilitate essential services and may need to vary between trips and markets or different product offerings or marketplace dynamics. They cover a range of services that promote safety and reliability, including the cost of building and maintaining technology interfaces, insurance, payment facilitation fees, technical assistance, security, onboarding and background checks for workers, marketing, or customer support, among other things. Specifically for digital platforms, regulating companies' service fees or mandating reporting requirements does not protect worker earnings or consumer affordability. Rather, it does the opposite, creating pressure to move costs like insurance and credit card processing fees onto consumers, thereby decreasing sales volume and adversely affecting worker pay. Further, regulating companies' service fees risks negatively impacting the level, pricing, and quality of the services provided.

Access to Talent

The modern workforce requires a flexible employment environment that allows workers to find opportunities that match their skills, interests, and availability. TechNet opposes efforts to eliminate or restrict this flexibility, including restrictions on remote and hybrid work, restrictions on opportunities for independent contractors and consultants, inflexible overtime rules, and indiscriminate expansion of collective bargaining rules. TechNet supports efforts to develop new avenues and safe harbors that empower companies to voluntarily provide new protections and benefits to workers where appropriate without impacting classification outcomes.

Sharing Economy

The sharing economy is creating income opportunities in every corner of the country, allowing people to work independently and on discretionary schedules, use their personal property and skills to generate income, help them expand their businesses, and provide for themselves and their families. Policymakers should ensure that efforts to regulate the sharing economy protect innovation and individual empowerment, are not overly burdensome, and recognize the unique nature of the sharing economy when compared to traditional providers.

As policymakers consider rules focused on the sharing economy, TechNet encourages policymakers to employ data-driven approaches to crafting policy that focus on the broader economic impact to communities and deemphasize the advocacy positions of legacy business interests. As the sharing economy continues to mature, TechNet encourages policymakers to consult relevant laws in guiding their policy decisions.

Portable Benefits

The composition of the U.S. workforce is changing as new technologies have provided low-barrier access to flexible, independent work. This type of work allows individuals and families in need of supplemental income, including during periods of unemployment or underemployment, to access work on demand. Over time, in large part due to the availability of new opportunities to offer services and sell goods, the independent income opportunities have increased and serve as an important source of supplemental earnings for millions of Americans.

Many in the modern, independent workforce find they get better financial returns on their skills than similar groups in the traditional workforce. Perhaps the biggest benefit to this new workforce is the flexibility that self-employment, independent contracting, and freelancing provide, which allows the independent workforce to balance work, family, and leisure activities differently than in a traditional employment relationship.

But the flexibility of independent work may come with challenges regarding access to important benefits and protections. The binary employment system forces workers to choose between employment with benefits but less flexibility, or independent contracting with flexibility but fewer benefits.

To address these challenges, state and federal policymakers are introducing policies to make it easier for independent workers to obtain and fund benefits. Policy solutions need to maintain the flexibility that workers who favor both online and offline independent work need and want, and they should weigh improving access to benefits for independent workers and their families. Because any such benefits must travel with the worker so they can continue to work independently for a variety of companies or individuals, the benefits must be portable.

Any portable benefits program should be guided by the following principles:

- Benefits should be tied to individual workers, enabling them to contribute to and use their benefits across multiple platforms or sources of income. Workers should also have flexibility over how to use their benefits.
- Programs should maintain the flexibility these workers seek while allowing technology companies to continue to grow and provide earning opportunities for more workers.
- Benefits should be proportional to the work completed, with more active workers receiving more benefits. Workers should also be able to make additional contributions to their account.
- Policy solutions should not limit technology companies' abilities to expand the benefits they offer to attract and retain independent workers.
- The program should incentivize companies to provide portable benefits to workers by establishing a safe harbor with respect to the independent contractor status of workers.
- The program should avoid duplicating existing requirements or creating unclear or confusing overlaps or conflicts with existing requirements.
- States should engage multiple stakeholders, including third parties, to establish a mechanism to manage portable benefits.
- Independent contractors deriving their benefits from a portable account should be eligible for the same kinds of tax breaks and pre-tax contributions as employees.

AUTONOMOUS VEHICLES AND CONNECTED VEHICLES

Autonomous Vehicles

Autonomous vehicles (AVs) enable tremendous societal benefits by improving road safety, increasing access to transportation for all, enhancing efficiency of goods movement, creating jobs, helping to reduce congestion, and meeting consumer demand, while promoting innovation and growth across various sectors of the economy.

Accordingly, TechNet supports policies that encourage the safe and efficient deployment of AVs on public roads in the United States. States should avoid adopting policies that will create, increase, or maintain barriers to the testing, development, and deployment of this technology and the benefits that come with it.

The state program supports the following principles:

- State policymakers should prioritize harmonization of laws between jurisdictions to avoid a patchwork of policies that may stifle or impede innovation. They should avoid establishing vehicle and equipment design and performance standards, safety regulations, or certifications that conflict with federal law, regulations, or guidance.
- State regulatory frameworks that restrict competition or limit operation of AVs to only one segment of innovators or automotive technologies should be avoided. Policies should be business model and technology-neutral and foster continued innovation in the industry, avoid picking winners and losers,

- prioritize public safety, and protect intellectual property.
- A human operator inside an AV should not be required. Policymakers should not predetermine how the technology will develop or legislate technology by specifying the role of a human in its development.
- Local ordinances, or other formal local sign-off, as a prerequisite for testing or deployment within a state should not be required. TechNet believes that a patchwork of local laws and regulations would be unnecessarily burdensome and could impede travel between jurisdictions.
- States should follow the guidelines and best practices outlined in the U.S. Department of Transportation's "Automated Driving Systems: A Vision for Safety 2.0" and "Preparing for the Future of Transportation: Automated Vehicles 3.0."
- The operation of AVs in a state should be subject to the same accident and operating reporting requirements as human-driven vehicles. Federal reporting requirements are sufficient to address the states' interest in assessing AV and road safety.
- State laws and regulations should be updated to remove legal barriers to driverless deployment of AVs on public roads, including vehicles with purpose-built designs.
- State policy should include the promotion of and investment in the broader AV ecosystem that supports accelerated AV deployments, including AV-related technologies, infrastructure, and other architecture that will enable and accelerate AV operations.
- States should promote policies that lead to a clear pathway to driverless commercial operations.
- TechNet also supports systems that promote access to publicly available data on road and traffic conditions.
- State policies should use definitions and terminology consistent with SAE J3016 (April 2021).
- Vehicles equipped with advanced driver-assistance systems (ADAS) are not AVs, and TechNet works to educate policymakers on the unique and distinct nature of both ADAS and AVs. State laws should prohibit vehicles equipped with ADAS from being advertised as AVs.
- States should avoid special or unique permitting, licensing, insurance, or registration requirements specific to AV operations.
- States should maintain existing laws on liability, unless and until the need for change is demonstrated.
- Bills and regulations should provide a clear path to the commercial, driverless deployment of AVs.
- Governments should not mandate the sharing of businesses' data that they cannot adequately analyze and use to promote further innovation.
- States should create a line of communication and provide industry expertise to various state AV task forces.
- Policymakers should avoid any regulations that limit or delay the use of AVs in public transportation systems. Limiting AVs in public transportation will deny mobility benefits to the riders that need it most.
- Policymakers should view AVs and related technology as job creators, with the AV industry playing a critical role in enhancing state and local economies, economic competitiveness, and opportunity overall.
- In general, policymaking should not form a distinction between AVs and human-operated vehicles unless there is a clearly articulable rationale.

Connected Vehicles

Connected vehicle technology has the potential to revolutionize transportation, making our roads safer, more efficient, and more environmentally friendly. TechNet supports policies that advance connected vehicle technology through investment in the research, development, and deployment of vehicle-to-everything (V2X) technology.

- States should partner with the federal government and private stakeholders to support the Department of Transportation's V2X Deployment Plan, including the near-, mid-, and long-term goals directed at infrastructure owners and operators.
- States should include V2X technologies in transportation budgets beyond pilot projects and demonstrations.
- States should, where relevant, include V2X in any roadway infrastructure plans or projects and any grant applications to the federal government.
- Public and private sector stakeholders, including federal, state, local, and tribal governments, as well as industry and research organizations, should collaborate and coordinate on connected vehicle policy, development, and deployment.

- States should support both Network and Direct V2X technologies, recognizing the unique ways in which both can contribute to safer roadways.

PROCUREMENT

TechNet seeks to promote and support innovation, transparency, competition, cost effectiveness, and technology neutrality in technology procurement processes. As states consider procurement reforms and legislation, TechNet will advocate for the following principles:

- Modernization of outdated IT systems, acceleration of the sound adoption of state-of-the-art technologies, and strengthening of state governments' cybersecurity defenses. Citizens deserve modern, citizen-centric services that keep pace with private sector innovation.
- Frameworks that encourage communication and collaboration between the public and private sectors to promote a better-informed understanding of current industry capabilities and practices.
- Strong executive-level leadership with supervisory and operational authority over enterprise-wide IT strategy, policy, and planning can drive innovation and maximize investment across state enterprises.
- Statutory flexibility to select from the widest array of solutions and consider all relevant factors in addition to cost, such as short- and long-term environmental impact and sustainability, the quality and security of goods and services purchased, performance history, and total cost of ownership solutions.
- Procurement and program management professionals benefit from training opportunities that expose them to technologies being deployed in the private sector.
- Reforms to standard contract terms and conditions to give agencies flexibility to use contracting vehicles that can accommodate the unique set of IT terms and conditions and incorporate future innovations that are aligned with commercial best practices.
- Reforms to allow for centralized procurement of managed services for the state or supported jurisdictions, which would achieve both efficiency and enable entities to acquire services they would not be able to if procuring on their own.
- Forced data localization requirements arbitrarily limit technology solutions.
- Opposing third-party verification and tracking software implementation requirements for vendors on state contracts.
- Intellectual property law should allow for an environment where innovation can flourish among companies of all sizes and across all sectors.
- Vendors should be held harmless when statute calls for stop payments due to agency failure.
- Vendors should not be discriminated against for policies which do not impact the delivery of technology solutions to the government.
- States should rely on federal laws and regulations related to international restrictions on contracting in lieu of enacting different, and potentially conflicting, state laws and regulations.

TAXATION

TechNet supports tax policies that promote innovation and foster an economic climate that enables companies to compete, thrive, invest, and expand in the United States and around the globe.

Due to many factors, the tax landscape at the state level is currently fluctuating at a rate not seen for decades. Research and development tax credits are popular in some states and under siege in others. Years of scarce budgets and underfunded infrastructure and public services are driving policymakers to consider new taxation schemes that will likely be counterproductive for long-term budgeting purposes. Meanwhile, new policy priorities in clean energy technology are creating opportunities for smart tax incentives.

TechNet's state program supports the following principles:

- Implementing research and development tax credits that spur growth in key technology sectors, including indefinite carry forward of research and development tax credits.
- Promoting decoupling of Section 174 required capitalization of research and development expenses allowing the continued or immediate expensing of such costs.
- Supporting legislation in the states to couple with IRC 168(k) Special Allowance for Certain Property (bonus depreciation).
- Supporting legislation to decouple current Section 163(j) interest expense deductibility limitations rules and replace with U.S. federal rules that existed for tax years beginning before 2022.
- Expanding access to existing tax credits for gig and sharing economy participants, particularly for products and services aiming to address real-life challenges such as accessibility, inclusion, congestion, and the electrification of transportation.
- Ensuring tax structures create a level-playing field for all product and service providers, both technology players as well as others, and do not disadvantage a specific subsector such as sharing economy companies and platforms where individuals can offer and pay for goods, services, or shared resources.
- Lowering corporate tax burdens and preventing attempts to raise corporate and payroll taxes in order to fund additional government services. Similarly preventing attempts by states to temporarily disallow deductions for prior tax losses (net operating loss) or utilization of tax credits legislation. These proposals disproportionately affect early-stage businesses that are growing into profitability.
- Preventing attempts by states to tax pre-written computer software and cloud computing services or software as a service (SaaS).
- Preventing attempts by states to apply broadly defined data processing and information services taxation regimes to an expansive set of technology-based applications and processes.
- Engaging on nexus tax legislation that negatively impact member companies and small businesses that are seeking to comply post-*South Dakota v. Wayfair*, including but not limited to marketplace facilitator nexus, economic nexus, payment facilitator nexus, remote seller representative nexus, and legislation using *Wayfair* to justify platform collection of locally administered taxes.
- Supporting policies that promote startup businesses by not increasing taxes on entrepreneurial investment activities.
- Promoting and expanding investment tax credits and angel investor tax credits.
- Supporting tax policy that provides clean energy technologies with a stable tax environment that appropriately supports the industry's unique financing needs.
- Finding an amenable and consistent way for states to tax or apply fees to the evolution of independent earning opportunities, which is rapidly growing and forcing policymakers to grapple with how to tax or apply fees to technologies that do not rely on brick-and-mortar presences in a state and are competing with traditional industries that already may be regulated and taxed.
- Ensuring any budget deficits at the state and city level are addressed with holistic strategies that do not disproportionately impact technology companies.
- Ensuring that any user fees are designed to provide digital platforms with flexibility on when and how the fee is assessed from the consumer in order to accommodate unique and innovative service models.
- Engaging against data excise taxes or the taxation of the collection of customer data.
- Engaging on digital tax legislation that discriminates against electronic commerce in violation of the federal Internet Tax Freedom Act.
- Engaging against retail delivery taxes or fees, which generally target online business models and harm delivery drivers, small businesses, and delivery-dependent households.
- Supporting language that excludes sales by affiliated entities on a common platform from the definition of marketplace and/or marketplace provider.
- Protecting user data by opposing government efforts to utilize platform users' tax information for non-tax purposes.

Priority Issues

Exempting Cloud/SaaS Taxes

Many states consider cloud or Software as a Service (SaaS) purchases as an untapped source of revenue as hardware offerings become less prevalent. The question centers on whether offering storage space in the cloud is a tangible "good" (subject to sales taxes), a "service" (subject to use taxes), or neither of those. Different

states are making different decisions and the situation is still evolving. TechNet will continue to advocate for national consistency and will oppose state-by-state efforts to extend traditional sales taxes to SaaS and related technology services to the extent that the imposition of such taxes has a disproportionately negative impact on cloud providers.

Marketplace Facilitator Collection

As states seek to revise legislation passed in the wake of the *Wayfair* decision, the state program will advocate for marketplace facilitator sales tax collection legislation that preserves a diversity of marketplace business models, especially with regard to the relationship between the marketplace facilitator and its customers and sellers. TechNet supports the principle that marketplace facilitators should be as free as possible – without creating a risk of under-collection of tax – to determine how to comply with marketplace facilitator collection requirements. To that end, TechNet will oppose legislation that allows marketplace sellers to unilaterally opt-out of marketplace collection. TechNet also supports the principle that sales are subject to tax only once. In addition, the law should be easy for consumers and marketplaces to comply with and for states to administer.

TechNet will also oppose efforts to extend marketplace facilitator collection requirements to other taxes and fees unless such collection is centrally administered by the state, changes are made to make such taxes uniform, and the state along with the help of localities provides information regarding such taxes on which platforms can reasonably rely. If a technology platform is deemed the retailer to collect taxes on a transaction, platforms should have the ability to collect and remit all such transactional taxes.

Investment Tax Credits

Legislation related to tax credits, such as research and development, employment credits for job creation, angel investor, venture capital, and technology investment/development tax credits, can spur growth, incentivize economic activity, and help companies make decisions regarding where to expand their operations. The current landscape for state-level tax credits is in flux. Traditional credits are embraced in some states but discontinued or in jeopardy in others. Increasingly, new tax credit proposals focus on the startup sector to ensure increased access to venture capital and angel investor dollars needed to succeed in a competitive market. TechNet will continue to educate policymakers about the benefits of smart investment tax credits, work to protect and/or restore traditional, existing credits, and promote consideration of new kinds of credits aimed at expanding the benefits into the innovation economy.

Clean and Renewable Tax Incentives

Many companies have a vested interest in “going green,” and consumers expect technology companies to be leaders in this endeavor. Furthermore, because of the global scope and nature of technology companies’ offerings, it is critical that they have a source of affordable, predictable, and reliable energy that will not be interrupted due to the myriad of political circumstances outside a company’s control. Lower energy costs allow tech companies to use those savings on other areas of their businesses. TechNet will promote the continuation and adoption of these incentives.

Oppose Digital Advertising Tax Legislation

As states grapple with how to tax the digital economy, we have recently seen proposals loosely modeled after the European Digital Services Tax policy that punitively target digital advertising. Working with the larger business community, TechNet will strongly oppose attempts to tax digital advertising. Advertising is merely a tool for generating sales and creating awareness of an issue, so it is unwise to impose taxes on these kind of business inputs and especially counterproductive in the current economic conditions where many small businesses that rely on digital advertising for messaging are struggling to survive. Besides being unsound policy, state proposals to date have contained vague definitions on the activity subject to tax and on sourcing methodologies which will lead to confusion for taxpayer implementation.

SMART INFRASTRUCTURE

In the near future, our infrastructure will blend traditional physical infrastructure (transportation and transit systems, buildings, pipes, power grids, concrete, and steel) with cyber infrastructure (computers, networks, and sensors), reaching the age of “connected everything.” Smart infrastructure is the development of more efficient and environmentally friendly systems for managing commuter traffic, food distribution, electric grids, services metering, waste management, street and highway lighting, and waterways. Transportation systems that are efficient, environmentally friendly, and move hundreds to hundreds of thousands of people quickly, comfortably, and affordably to their destinations will be a defining feature of many new smart cities.

TechNet recognizes that a sustainable and equitable transportation system requires people to be able to access a variety of transportation options and choose the one that is best suited to their task, which often will not be a personally owned vehicle. TechNet supports efforts to incentivize expansion and use of alternative mobility options, including peer-to-peer car sharing, ridesharing, autonomous vehicles, and micromobility.

Tomorrow’s smart cities will redefine sustainability and livability. The common thread for these smart infrastructure technologies is the reliance on a high-speed — wired or wireless — internet connection, including 5G.

In order to execute these smart solutions, there remains the need to keep pace with the explosive pace of technological innovation. The state program will support legislation that promotes research, development, and investment in smart infrastructure and modernizes archaic regulations allowing companies to create and meet the increased demand of consumers, cities, and government agencies, while ensuring that there is an even playing field in terms of technological adoption and innovation.

The state team will advocate to ensure that infrastructure policies, such as zoning and building codes, are future-proofed. In addition, infrastructure policies should support energy efficiency, renewable energy, transportation electrification, and public-private partnerships designed to facilitate infrastructure improvements.

Broadband and Internet Access

The internet is a key tool for consumers’ access to information and empowerment. Internet access connects consumers with the tools they need to live a more flexible lifestyle, increasing their access to telehealth, remote education, civic engagement, provision of government services, and allowing for workplace flexibility. Embracing policies that close the digital divide and expand access to the internet and technology, provide a safe and secure consumer experience, and promote strong private sector competition and investment (while opposing provisions that would create unnecessary or burdensome regulations or legal requirements) is a core value of TechNet. TechNet will support efforts to increase and expand high speed broadband deployment to currently unserved areas and increase adoption by encouraging private investment and making government funding competitively available to all providers for those hard-to-serve areas where private investment on its own is not sufficient.

APPENDIX - ENERGY

Priority Issues

Demand Response (DR)

TechNet’s members include “clean tech” companies that offer DR products, companies that are energy

customers who utilize DR programs as part of their energy portfolio, and companies that have to meet DR requirements due to state regulations or as part of their own internal environmental stewardship programs.

TechNet will support policies related to electric demand management, including but not limited to peak demand reduction standards and incentive programs, DR requirements for energy consumers that educate the consumer, better management of energy loads, and improvement of the efficiency, resilience, and effectiveness of the energy supply chain.

Distributed Energy Resources (DER)

Distributed Energy Resources (DER) are electricity generating or load reducing/managing resources that are deployed across the distribution grid, typically close to load, and usually behind the meter, which can be used individually or in aggregate to provide value to the grid, individual customers, or both. DER may include distributed generation (DG), on-site generation, energy efficiency, distributed renewables, behind-the-meter resources, energy storage, and load control/management.

Distributed energy resources must be a key component of a state's clean energy portfolio and grid modernization efforts. As with demand response, DR is of interest to both TechNet's "clean tech" companies who offer DER products and services and to those customers who have invested in DG onsite and utilize DERs as part of their energy consumption and management portfolio.

DER and energy management tools can help meet onsite customer energy needs and provide wholesale, grid-facing services, either individually or in aggregate. DER, deployed effectively, can reduce utility and customer costs, improve service reliability and safety, and enhance grid resilience while achieving climate and environmental goals. TechNet monitors all types of DER, such as onsite generation and storage, energy efficiency, demand response, and advanced energy management technologies, including smart thermostats and intelligent appliances.

TechNet will support legislation, regulations, and executive actions that encourage and support the use and expansion of DERs as part of the overall energy supply and minimize or eliminate barriers and costs to interconnect DERs to the grid.

Energy Efficiency Standards

TechNet supports efforts to promote energy efficient technology adoption and the development of new energy efficient technologies. TechNet believes that states should rely on voluntary industry standards rather than imposing state-specific regulations to improve energy efficiency, as consumers may be confused by a patchwork of state regulations for products that are supplied on a global scale. Current energy efficiency standards are generating significant energy savings and adoption is widespread across the electronic product spectrum.

Resilient Energy Supply

The technology sector is increasingly dependent on an uninterrupted supply of electricity. At the same time, climate change, extreme weather events, and security threats to the electric grid are growing. TechNet and its members recognize the value of electricity supplies that are able to ride through outages of the electricity distribution system and/or restore the distribution system more rapidly after an outage. TechNet supports policies and programs that recognize the value of resilience either in the form of stand-alone policies or as features of existing programs. TechNet understands that clean energy and resilient energy are not mutually exclusive and will seek to advance the interests of its members by advocating for policymakers to enhance their focus on the intersection of sustainable energy and resilient energy.

Clean Energy Standards, Renewable Portfolio Standards, Alternative Portfolio Standards, Renewable Fuel Standards, and Low Carbon Fuel Standards

In order to address climate change and reduce air pollution, many jurisdictions have adopted Clean Energy Standards (CES), Renewable Portfolio Standards (RPS), Alternative Portfolio Standards (APS), Renewable Fuel Standards (RFS), and Low Carbon Fuel Standards (LCFS), which are requirements or incentives to ensure that

energy marketers and producers have a certain percentage of clean energy in their mix. There are obligated parties when it comes to clean energy standards, and it is critical that we understand when there is a change in law related to these standards.

TechNet is interested in the trend of states setting clean energy portfolio and renewable fuel standards for customers and market participants. In addition, some TechNet members offer products and services to help customers, energy companies, and states achieve the RPS, CES, APS, LCFS and Environmental Protection Agency (EPA) RFS mandates. Beyond this, we support the development and investment in alternative fuels including, but not limited to green hydrogen and biofuels, to reduce carbon emissions from our existing fuel sources.

TechNet will engage for CES, RPS, APS, LCFS, and RFS goals in conjunction with open access to both grid and consumption data. We will advocate to ensure that the approach is practical, technology-neutral, and compatible with member companies' procurement goals, the evolution of renewable development, and the innovation of sustainable market solutions. We will advocate for the recognition, when determining compliance with state CES or RPS, of member companies' accelerated voluntary purchases of renewable energy to ensure member companies are not paying twice for renewables while also lowering the overall cost of compliance for all utility customers.

Grid Modernization

TechNet defines grid modernization as addressing the needs of the aging grid to meet the needs of customers, such as using communications and modern computing to upgrade the current electric power grid and leverage DERs and grid-enhancing technologies (GETs) so that the electric grid can operate more efficiently and reliably and enable additional services to consumers. Modernization makes a grid into a platform on which market-based solutions can thrive, delivering more value and savings to consumers and reducing carbon dioxide emissions. To meet this end, grid modernization policies must include technologies and standards that enable customer data access and allow customers to easily share data with third parties. Additionally, grid modernization should be supported with integrated system planning at the distribution, transmission, and bulk power system levels to ensure that the power grid can continue to support customer adoption of clean energy technologies, as well as ensure that these resources are being fully utilized to address grid needs.

Transitioning to an integrated system planning process will require greater data transparency regarding planned investments and system constraints driving those investments. The transition will also require changes in how the utilities identify and pursue solutions to address system constraints to ensure they are considering the so-called "non-wires alternative" in lieu of the more conventional investments they would otherwise rely upon.

TechNet will monitor and advocate for grid modernization policies or incentives, as well as promote policies to reform utility planning processes to take a more integrated approach. TechNet will monitor policies to ensure that grid modernization policies and proposals will truly reflect the definition of grid modernization and do not pass unnecessary or unjustified costs onto consumers.

Retail Energy Competition and Self-Supply

Retail energy competition is when a state authorizes energy (electricity and/or gas) purchases from a supplier outside of the monopoly utility provider. Self-supply allows a consumer to procure their electricity needs outside traditional utilities. TechNet believes that competition and self-supply allow for and encourage innovation. Allowing customers the flexibility to procure power and gas from a source other than the monopoly utility allows the customer to incorporate clean technology, procure cost-competitive renewable energy, and tailor energy to the needs of their facilities and organization. Typically, energy costs are among the top three highest expenses for businesses. Controlling these costs is critically important, and retail competition and self-supply empower customers to better manage energy costs.

TechNet will support policies that encourage retail choice, energy competition, or consumer self-supply and advocate for an even playing field for all suppliers, including the incumbent investor-owned utilities. TechNet will oppose any additional requirements imposed on suppliers and customers as prerequisites to participate in competitive energy markets.

Grid and Customer Data Access and Transparency

In the energy space, customer data is the foundational element of every business that directly touches customers and a number of businesses that operate more at the wholesale level. The entity that controls customer data has a huge impact on the success or failure of those businesses. In the traditional utility model, the entity that owns the metering infrastructure (which, for all relevant U.S. jurisdictions, is the utility) is the *de facto* owner of the data. Even customers, who may technically be considered (by law or regulation) the beneficial owner of the data, must get their data from the utility, which typically has the right to retain the data and use it for many purposes.

This model of utility-owned data seriously limits the value that customers can derive from the market. A third-party supplier's ability to offer (and bill) advanced products and services will also be limited by the quality of the data that is passed from the utility to the third party. There can be a material difference in data quality between what the utility sends to a third party and what the utility actually gathers at the meter level and/or sends to the system operator for settlement purposes. At the same time, as customer adoption of DERs increases, distribution system planning and operations will require additional data and information for grid operators and DER providers. Therefore, in order to realize the promise of a modernized grid, the underlying data associated with the grid must be made available to a wide group of industry stakeholders and market participants while maintaining appropriate consumer data privacy. Furthermore, the inconsistency of data standardization from electric utilities creates hurdles for customers with multi-state operations and third-party DER providers.

TechNet will advocate for expanding the boundaries of access to data and customer choice and will encourage legislators and regulators to consider several possible changes to their current system. TechNet will also advocate for the use of a standardized format for providing customers and third-party providers with data on a consistent format.

Electrification of Transportation

Electrification of transportation includes all electric vehicles (EVs) including medium and heavy-duty, electric vehicle supply equipment (EVSE), charging stations, and related smart and networked software solutions. EVs include all technology types, including battery EVs, plug-in hybrid EVs, and hydrogen fuel cell EVs.

Charging and hydrogen fueling stations are being installed throughout the country along corridors, in urban hubs, at businesses, delivery fleets, public lots, and in residences to fuel electric and fuel cell electric vehicles. While the industry has grown significantly as EVs have become more widespread, stakeholders generally agree that there is a need to accelerate deployment across the light, medium, and heavy-duty sectors. State agencies and electric utilities are now considering ways to accelerate charging and hydrogen refueling station deployments and fueling switching. Utility rate-basing of grid upgrades to support EV charging and utility-owned-and-operated charging stations can support transportation electrification but must not threaten competition and innovation in the charging station industry. The EV charging market will continue to thrive as more EV models are introduced, hardware costs decrease, installations become more streamlined through enabling building codes, and station utilization improves. However, states can take targeted action to spur greater investment to close the infrastructure gap and support diverse networks of charging and hydrogen refueling stations.

Utilities have proposed a variety of approaches to directly participate in supporting the development of EV charging infrastructure, from utility-owned and operated infrastructure to "make ready," which is the infrastructure needed to install a charging station, up to but not including the station itself.

TechNet will respond to utility applications at the relevant public utility commissions where investor-owned utilities are seeking to rate-base charging infrastructure, and TechNet will support proposals that help accelerate the electric vehicle sector while respecting customer choice, long-term competition, and innovation in the EV charging market. Moreover, TechNet will advocate for customer control and choice, technology-neutral hardware and software options, and competition in the EV charging marketplace.

TechNet will oppose efforts to require EV manufacturers buy back or compensate dealers for the cost of a dealer's investments in EVs.

As more public funding becomes available, TechNet supports robust and flexible incentive programs, not mandates, that accelerate EV adoption and charging and hydrogen refueling infrastructure among individuals and fleets for light, medium, and heavy-duty vehicle classes alike. These programs should offer opportunities for funding for different types of EV technology and prioritize supporting private market solutions and transportation modes with the greatest potential impact to electrify both a high quantity of vehicles and high-mileage applications, including personal, fleet, ridesharing, ride-hailing, autonomous vehicles, transit, micromobility, peer-to-peer car sharing, and more.

Clean Energy Supply

TechNet members are financing, building, and innovating on clean energy projects. These projects are needed to meet growing demand and help deliver economies of scale to the energy markets. Additionally, these projects help spur economic development in many communities. Many states have incentives and streamlined permitting processes to facilitate the development of these projects. However, some states have created artificial barriers through legislative and regulatory changes that have slowed investment. TechNet will advocate for a policy environment that advances efforts to bring more clean energy projects online more quickly or extend the useful life of existing clean energy projects.

Microgrids

Microgrids are localized grids that can disconnect from the traditional grid to operate autonomously and help mitigate grid disturbances and strengthen grid resilience. Microgrids can play an important role in transforming the nation's electric grid in the face of continued threats from climate change and natural disasters. In addition, they can function as a grid resource for faster system response and recovery.

Microgrids also support a flexible and efficient electric grid by enabling the integration of growing deployments of renewable sources of energy such as solar and wind, distributed energy resources such as fuel cells, energy storage, and dispatch, and DR. In addition, the use of local sources of energy to serve local power loads helps reduce energy losses in transmission and distribution, which further increases the efficiency and resilience of the electricity delivery system.

TechNet members are financing, building, and innovating in the area of microgrids, and TechNet will advocate for policies and programs that encourage microgrid development.

Demand Charges

Today, many utilities assess demand charges to some commercial and industrial customers, and some are proposing mandatory demand charges for residential or distributed generation customers. This is a concern for DER providers and EV charging operators because demand charges can reduce the price signal for residential customers to adopt these technologies and can make a customer's bill much more complex because of the charges' many facets and various ways in which they can be applied.

TechNet will advocate for preserving customer choice and the option to utilize and invest in the variety of available advanced energy technologies from both the residential and commercial customer perspective for DERs in the rate design discussion. TechNet will support utilities exploring optional rates, including time variable rates and pilot programs that send clearer signals about system costs that enable technology innovation and customer control over energy costs. On the commercial side, TechNet will support transparency in demand charges and demand charge alternative tariffs. Specific to EV charging, TechNet will advocate for considering alternate rate design options for demand charges to respond to increased adoption of EV and higher power technology.

Special Contracts

Today, many utilities have the authority to enter into special contracts with commercial customers to enable load growth, encourage state economic development, and ensure no impacts on other rate classes such as residential customers. TechNet will advocate that all utilities have the authority to enter into special contracts that enable new energy supplies, expand the grid, encourage economic development, and ensure other ratepayers are not impacted.