

THE FUTURE OF TECH: A BLUEPRINT FOR ACTION

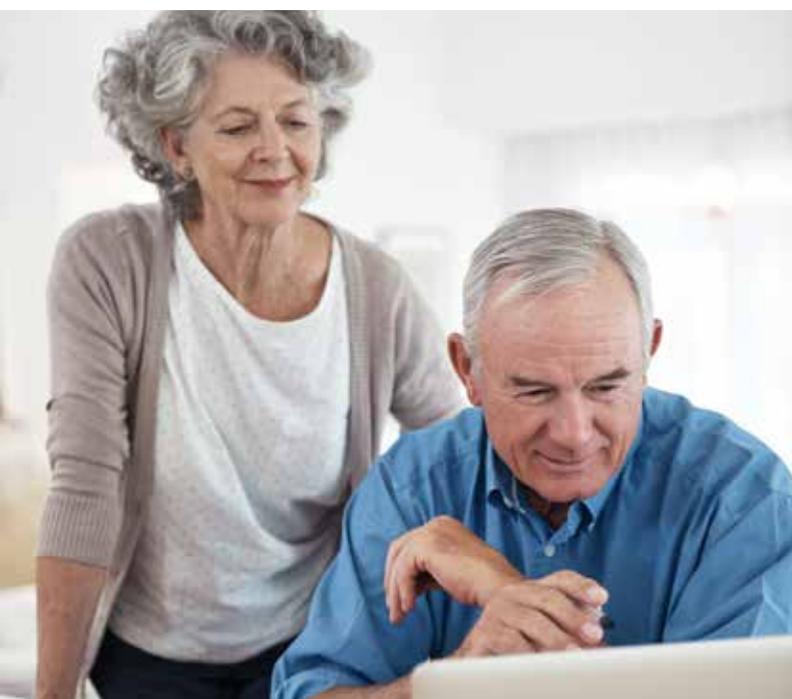


TABLE OF CONTENTS

A Message from the Commissioners	1
Executive Summary	5
An Agenda for Action	12
Protecting Your Information, Your Privacy, and Our Democracy	15
Hardening America’s Cybersecurity	24
Ensuring Open and Competitive Markets	28
Sustaining America’s Leadership in Innovation	32
Appendix	37
About the Commissioners	37
Town Hall Locations and Partners	38
Interview and Town Hall Participants	39
Future of Tech National Polls	43
Acknowledgements	53

A MESSAGE FROM THE COMMISSIONERS

On any given day, millions of Americans wake up to an alarm from a smartphone. They check their email and text messages, and scroll through social media for the latest news on national or world events, or the activities of friends and family. They post comments on and reactions to what they see or hear.

On any given day, students receive, prepare, and submit their homework remotely. During the COVID-19 pandemic, millions of students have attended classes virtually while their parents worked online, exchanging messages and ideas through chat services or video conferences. Businesses regularly recruit and hire talent to work remotely, and many business leaders and workers alike expect that remote or hybrid work will be the norm going forward.

On any given day, whether working in offices or at home, Americans design fashion lines, housing and office towers, roads and bridges or video games, and launch business ventures and nonprofits online.

On any given day, Americans go to the web or a mobile app to buy a birthday or wedding gift, order groceries or business supplies, book a trip, order a rideshare or a meal, find directions, pay bills, deposit checks, invest money, or apply for a job. Seniors apply for Social Security and Medicare benefits online. Many Americans get essential health services—from routine to urgent to mental health care—through telehealth platforms. In a few states, Americans vote online.

And at the end of any given day, Americans stream a movie, play games online, or swipe for a date—or return to sending emails and text messages and posting commentary on social media.

Technology is everywhere.

For more than fifty years, the United States has led the world in life-changing, often life-saving technology.

Technology is everywhere. For more than fifty years, the United States has led the world in life-changing, often life-saving technology. Public investments in basic research led to the creation of the internet, which in turn spawned private innovation, jobs, efficiencies, and breakthrough advances in education, health, engineering, communications, entertainment, public safety, and commerce. These innovations have enriched and enabled the lives of hundreds of millions of Americans and people all around the world. They are the engine of our global economy.

The ubiquity of technology in our lives, society, and economy demands that the U.S. develop a **coordinated national technology strategy.**

At the same time, on any of these given days, in rural and urban communities alike, millions of Americans either lack or cannot afford the essential tool to perform all these tasks—high-speed internet. As many as sixteen million American children have no online access to do their homework or the research to complete it. Millions of small businesses lack a basic connection to the markets, customers, and suppliers that proliferate online, stifling job creation and opportunities. Millions of families cannot get the affordable, quality care or the answers they need through telehealth, because they have no high-speed broadband.

For those who do have access, every click of the mouse—every internet search for information about a job or research paper, every news item we scroll through, every movie we stream, every item or service we order online—produces personal data about our interests, likes and dislikes, environs, locations, and associations. That data is then harvested—often without our knowledge—and bundled for advertisers (who target us with things to sell), politicians (who target us with personalized fundraising or get-out-the-vote and policy appeals), and sometimes other companies, law enforcement, and foreign governments (who track us). Sometimes that information is stolen and used by sophisticated criminals, here and abroad, to commit fraud or threaten our children's safety. Sometimes it's deliberately used to stoke our outrage (and online engagement) by trapping us in an information echo chamber that serves to confirm or, at worst, to control our own views. And sometimes it is used to spread lies, ranging from misinformed but ultimately harmless rumors to harassment or disinformation designed to jeopardize public health, national unity, or democracy itself.

On any given day, individuals, as well as companies and organizations—including manufacturers, utility operators, banks, hospitals, universities, government agencies, and the military—are attacked by cyber scams, phishing, malware, and other online tactics to hack, disrupt, disable, or otherwise gain access to critical operations and data.

Today, the ubiquity of technology in our lives, society, and economy, and the impact it has on democratic engagement and function, demand that the United States develop a coordinated national technology strategy that establishes national standards and boundaries to protect the safety of America's children, families, businesses, consumers, and the public good, while ensuring that we maintain our edge in technological innovation.

Recognizing the urgency of these challenges and opportunities, the independent, nonpartisan Future of Tech Commission was formed to consider and propose a national framework and tech policy blueprint for the United States. To that end, the Commission convened 11 town halls; engaged approximately 150 experts, industry and thought leaders, and advocates and over a thousand citizens from across the country through town halls and interview discussions; commissioned a nationwide poll of more than 2,000 registered voters; and reviewed scores of relevant articles and books to fully understand the challenges we face and to hear a variety of proposed solutions. On the basis of that widespread input and analysis, we now offer this report and these proposals to the Administration, the Congress, and the American people.

We have not presumed to opine on every issue presented by the many applications of technology in our lives. However, based on the range of input and information shared with us, it is clear that there is broad consensus on a few key points, namely that:

- Every American **should have access to affordable broadband internet services** at home, school, and work. The recently enacted bipartisan infrastructure legislation is a historic step.
- Every American **should be protected from the misappropriation** and misuse of their and their children's personal data; from misinformation and disinformation that threaten public health, safety, and a flourishing democracy; and from infringement of their freedom of speech online, a fundamental American value.
- Every American **should be able to depend on an online market of products and ideas** characterized by safety, security, consumer choice, transparency, affordability, quality, and innovation.

Americans everywhere understand that universal broadband internet access is as essential to the average American today as electricity and water. They also appreciate the importance of broadband that is reliable, safe, modern, trustworthy, and affordable.

Experience has shown, however, that the private sector has not and will not meet the objectives listed above on its own. Experts agree that there is an urgent need for government at all levels to address these interests, and that state-level and local undertakings alone are insufficient. Indeed, since our work began, industry leaders themselves have called for federal regulatory intervention.

We believe that it is imperative for America to develop a coordinated national framework and tech policy blueprint. In some cases, the objectives will be best served through partnerships between the federal government and the states, or between the public and private sectors. In other cases, the federal government should exercise its singular responsibility to legislate and regulate for the public good. Above all, we must act now.

Americans on a bipartisan basis overwhelmingly agree that action is needed urgently. According to our nationwide poll, conducted in late summer of 2021¹:

- 89 percent of Americans agree that **understanding how to use technology is essential for most of our workforce.**
- 82 percent agree that **we need universal access to high-speed internet to ensure our kids get the education they need to compete and win in a global economy.**
- 80 percent agree that **the federal government must do everything it can to curb the influence of organizations that have grown too powerful and now use our data to reach too far into our lives.**
- 88 percent agree that **tech companies should be required to ask consumers whether or not they can use their data.**
- 88 percent agree that **one of the biggest threats to our national security is a data breach by foreign adversaries.**

Our most recent poll, conducted in February 2022, reaffirmed these findings from Republican, Independent, and Democratic voters: **76 percent of Americans support restricting companies from collecting and using personal data beyond what's needed for effective service, and 75 percent agree that if the United States does not establish rules and guardrails around dangerous or false content online, our democracy could be under threat.**

We clearly need a thoughtful, coordinated national policy that serves the values that Americans share and ensures that our country will continue to lead the world in technology and innovation. We believe that we are up to this task, and it will take all of us.

We have a history of successfully leveraging personal and industry ingenuity and creativity with public leadership and investment. In the 1930s, for example, the Rural Electrification Act brought electricity to farms, improving working and living conditions for millions of rural Americans. In the 1950s, the National Interstate and Defense Highways Act created the interstate highway system—the largest public works project in American history at the time—bringing prosperity, opportunity, and connection to much more of the country. In the 1960s, after President Kennedy announced the ambitious goal of landing a person on the moon and returning that astronaut safely to Earth, we accomplished that historic feat with the flight of Apollo 11 in 1969. Americans came together in the wake of 9/11, creating the Department of Homeland Security to tackle foreign terrorism and threats. And bipartisan cooperation in 2021 resulted in passage of the Infrastructure Investment and Jobs Act, a once-in-a-generation investment in our country's infrastructure and competitiveness. We have won world wars, created and transformed industries, and forged a future by unifying around a common purpose, with contributions from every sector. We can do this again by creating and implementing a coordinated technology infrastructure and consumer environment that is worthy of our highest values and fit to help shape our children's future.

Signed, Margaret Spellings, Deval Patrick, and Jim Steyer

¹ Benenson Strategy Group, July 2021, <https://www.bsgco.com/post/voters-want-to-curb-the-influence-of-big-tech-companies-new-poll-shows>.

The strength and breadth of our tech industry is a powerful American advantage. Our muscular, innovative, next-level companies have created millions of jobs and incalculable value with tools that enable us to connect, work, learn, shop, play, inform each other, access financial and health services, and unlock extraordinary opportunities and economic potential. Through technology, American productivity has soared. We do not want to see that asset hobbled.

Americans depend on and embrace these tools, but they also see their perils and pitfalls—from privacy issues and the amplification of harmful mis- and disinformation to threats to our children’s safety and the very functioning of our democracy.² Today, there is widespread agreement among Americans that we must urgently address the vast impact of technology on our society with a coordinated, common-sense approach.

The independent, bipartisan Future of Tech Commission was formed in April 2021 to investigate these challenges and propose a coordinated tech strategy for the United States. We specifically considered issues of universal access; data privacy and the related issue of platform safety; cybersecurity; market competition; and technological innovation.

Between April and December 2021, we held mostly virtual town halls around the country—in Arizona, northern and southern California, Connecticut, Florida, Indiana, Massachusetts, North Carolina, and Texas—and two in Europe. We interviewed dozens of industry leaders, experts, and advocates in the U.S. and abroad and invited direct input from citizens. We also conducted comprehensive public opinion polls with thousands of registered voters nationwide in late summer 2021 and early 2022, which revealed remarkable findings about the American public’s attitudes toward technology policy.

There is strong bipartisan agreement that the government must play a role—as it does, for example, in ensuring the safety of our food and water—by establishing safeguards to protect consumers’ privacy, minimize mis- and disinformation, and strengthen our nation’s cybersecurity. In addition, Americans want to maintain our global leadership in technology, research, and innovation. This blueprint seeks to set that course.

² Misinformation is false, misleading, or out-of-context information that is presented as fact without the intention to deceive. Disinformation is misinformation that is deliberately spread with the intent to deceive or mislead.

In the body of this report, we detail proposals in several areas we explored, with the exception of universal broadband service. Universal access to reliable, affordable, high-speed internet is clearly foundational, and there is broad consensus that all Americans must have it to participate fully in our society. Fortunately, in November 2021, Congress passed and President Biden signed the bipartisan Infrastructure Investment and Jobs Act, which includes \$65 billion for broadband infrastructure deployment and adoption to help make high-speed internet access a reality for every American. This would have been a central recommendation of the Commission.

Now that Congress has allocated the needed funds, the Administration should commit to closing the digital divide and making broadband universal within five years through

timely, accountable implementation at the federal, state, and local levels; accurate, up-to-date mapping; and robust oversight. Through effective policy implementation—ensuring that high-speed internet access is available, affordable, and adopted in every urban, suburban, rural, and remote community, in every home, and in every workplace—technology can be a great equalizer of access, education, and opportunity for all our people. It can also close the “homework gap” for millions of schoolchildren. This gap existed for years, but it became an even greater problem during the COVID-19 pandemic. When schools closed across the country, too

many students without adequate internet access resorted to sitting in library and school parking lots to use those buildings’ free Wi-Fi to do their homework.

Below, we propose muscular congressional and executive actions that will strengthen protections for all Americans; require transparency from tech companies; bolster our nation’s ability to respond to and prevent cyberattacks; and foster innovation, competition, and consumer choice. We summarize them as follows:

“I compare this moment to something Dwight Eisenhower observed as a young military officer—that America’s roads and bridges and tunnels were not fit for the transportation needs of the military. It’s a lesson he never forgot. And in 1956, President Eisenhower signed the interstate highway act into law in America.

That’s how profoundly we need to improve our technology infrastructure today.”

—Jeb Bush, former governor of Florida

PROTECTING YOUR INFORMATION, YOUR PRIVACY, AND OUR DEMOCRACY

Whenever we connect, the apps and platforms we use collect sensitive information about us, including our habits, hobbies, locations, interests, and friends. That information is often used to target us with products, opinions, brands, and political ideas. Many of us are not aware that this information is tracked, collected, bundled, sold, and used or misused. The often-dense privacy policies of the apps we rely on do not help us better manage our privacy. Some apps even track minors without their parents' permission.

Online targeting—using harvested personal data—is also directly related to the assault in recent years on our sense of shared reality. Social media has brought many people together around the world. It has also, however, increased the reach and velocity of lies and destructive narratives by spreading misinformation from a variety of sources—including websites, cable television, and online influencers.

While our Constitution guarantees freedom of speech, it does not guarantee freedom of reach.³ Illegal, harmful, or misleading content, amplified algorithmically to millions of people online, has undermined public health, promoted violence, and jeopardized our democratic system.

We believe that these practices must end. Just as we regulate our food system to protect the public's health and safety, it is time to set common-sense standards to protect our privacy and personal information and curb the amplification of mis- and disinformation. Accordingly, we recommend that Congress and the Administration:

- Pass a comprehensive **Federal Privacy Law** that gives consumers control of their privacy and requires companies to implement policies of data minimization with respect to personal data collection and use—i.e., restricting their collection and use of data to what they require to provide their services.
- Pass a powerful new **Children's Privacy Law** that updates and strengthens protections for children and teens.
- Enact clear, understandable **transparency requirements** with respect to the use of algorithms, and other reforms, to rein in tech platform practices that harm children, families, public health, national security, and democracy.
- Create a **Public Interest Media Fund** to invest in trusted local sources of news and information—which social media companies have played a role in replacing—that is financially supported by tech companies, a percentage of money from FTC fines on tech companies, and/or a merger transaction fee.

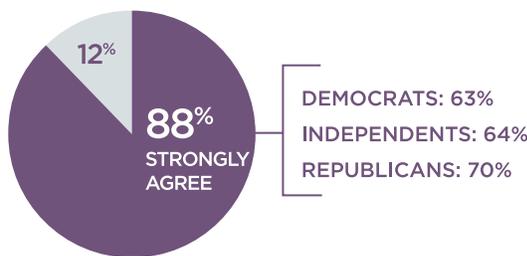
³ Renee DiResta, "Free Speech Is Not the Same as Free Reach," *Wired*, Aug. 30, 2018.

We also believe that the White House should leverage existing regulatory authority by coordinating departments and agencies to:

- Address critical **privacy and data protection** needs, and
- Enforce other **consumer protection and anti-discrimination rules** in the context of online behavior.

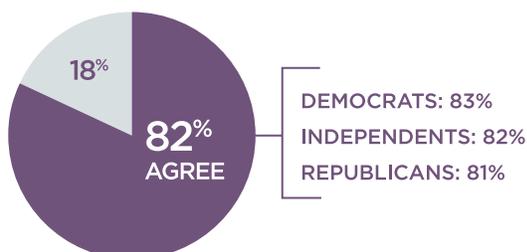
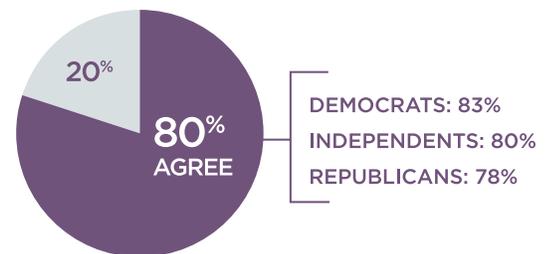
To that end, we recommend that the White House:

- Establish a **White House Technology Coordinating Council**, with clear and paramount authority to develop, coordinate, and help drive progress on a national tech policy strategy.



Two-thirds (88%) of voters strongly agree that **tech companies should be required to ask consumers** whether or not they can use their data.

80% of voters agree (42% strongly agree) that **the federal government needs to do everything it can to curb the influence of big tech companies** that have grown too powerful and now use our data to reach too far into our lives.



82% of voters agree (41% strongly agree) **after years of unchecked growth, we need to do more to regulate big tech.**

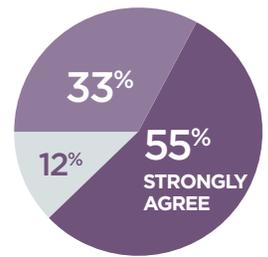
HARDENING AMERICA'S CYBERSECURITY

Cyberattacks are a fast-rising threat to individuals, businesses, and government. These attacks—some perpetrated by foreign state actors—can damage U.S. industry, critical infrastructure, and even hospitals and schools. Many Americans have been victims of online crimes, including identity theft, hacking, phishing, malware, and ransomware. Governments at the local, state, and federal levels have experienced breaches in systems ranging from those that provide safety-net services to those that involve our military defenses.

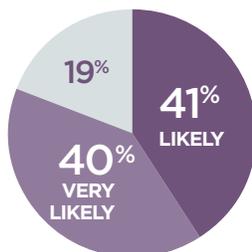
We need to prevent cybercrime, improve our preparedness, and develop the most effective responses to cybersecurity threats. Accordingly, we recommend that Congress and the Administration:

- Establish proactive **Regional Cybersecurity Centers**—consisting of both public and private actors across critical industries—to support real-time public/private coordination, rapid response, and prevention efforts against personal and industrial cyberattacks.⁴
- Give greater consideration to **ransomware reporting and breach notification requirements**, acknowledging the need for timely information, coordination, and transparency when a breach occurs.
- Support the **deployment of additional resources** in the Defense, Homeland Security, and Justice Departments—as well as in the intelligence agencies—to harden our networks and strengthen our national security capabilities.

55% of voters strongly agree (88% total agree) that **one of the biggest threats to our national security is a data breach by foreign adversaries.**



⁴ The Cybersecurity and Infrastructure Security Agency (CISA) currently has 10 regional offices to support the security and resilience of critical infrastructure owners and operators and state, local, tribal, and territorial partners (<https://www.cisa.gov/cisa-regions>).



National cybersecurity is a top priority for voters, who overwhelmingly believe a foreign cyber attack is imminent—81% of voters believe it is likely (40% very likely) that **in the next five years the United States will be a victim of cybercrime**, where the country's critical infrastructure is hacked by a foreign adversary.

ENSURING OPEN AND COMPETITIVE MARKETS

We believe that America deserves a market for internet technology and services that is second-to-none, conducive to investment, innovation, job creation, and entrepreneurial entry. We believe such a market serves the needs of consumers, small businesses, and entrepreneurs and strengthens our international competitiveness in a fiercely competitive global economy. The Department of Justice, Federal Trade Commission, and several state attorneys general are actively engaged in antitrust investigations, litigation, or other enforcement actions in this area. We are sensitive to involving ourselves directly in such ongoing actions and inquiries. Congress, meanwhile, is seriously considering new antitrust legislation aimed at increasing the authority and tools available to antitrust enforcers.

The Commission does believe, however, that the U.S. is stronger and the marketplace healthier when markets are open, fair, inclusive, and fully competitive. We also acknowledge the global supremacy and scale of American innovation. Accordingly, the Commission recommends and supports:

- Efforts by the Administration, Congress, and state attorneys general to **enforce our nation's competition laws** as well as reinforce our nation's commitment to fair and open markets by strengthening the tools of regulators and antitrust enforcers.

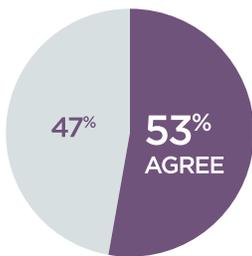
Beyond that, the Commission believes that we can give consumers power, choice, and control over the content that they see, create, and share across different platforms by **passing a comprehensive Federal Privacy Law**, as recommended in this report. In addition, the Commission recommends that Congress and the Administration:

- Expressly authorize and enable local government and community organizations and companies, such as cooperatives and municipal broadband providers, to **compete for existing and expanded service** as a means to help lower broadband prices for consumers and expand consumer choice.



DEMOCRATS: 86%
INDEPENDENTS: 81%
REPUBLICANS: 81%

A strong bipartisan majority of American voters—83%—support enacting **regulations that enable a competitive, affordable broadband market.**



DEMOCRATS: 50%
INDEPENDENTS: 55%
REPUBLICANS: 56%

A majority of voters—53%—on a bipartisan basis agree that a handful of very large companies dominate the sector, **making it very difficult for new companies or start-ups to compete.**

SUSTAINING AMERICA'S LEADERSHIP IN INNOVATION



9 in 10 American voters agree that **technological innovation will transform the way our kids live, work, learn, and connect with each other**, with 55% strongly agreeing.

For more than 30 years, the United States has been a global tech leader. Public investment in basic scientific research spawned the technology revolution, including the internet, GPS, smartphones, search engines, and many other innovations now central to daily life. For America to maintain its leadership, the Commission believes we must develop coordinated tech policies that safeguard privacy, defend open markets and national security, and continue to safeguard our democracy.

Many countries have already passed national privacy laws, creating a worldwide patchwork of regulations with which global U.S. companies must comply. The absence of a national privacy law in the United States makes doing business more complex and the internet unsafe for many individuals. This absence can also erode trust in American products, since buyers may lack faith in their adherence to privacy-protection principles.

Meanwhile, our public investment in basic research has dropped significantly, threatening our ability to develop groundbreaking innovations in the future while other nations race ahead. And new technologies, such as artificial intelligence (AI), are expanding rapidly without ethical guardrails that address the public interest in personal safety, national security, and nondiscrimination.

We believe the recommendations in this report will enhance the environment for tech innovation in the future. In addition, we recommend that the White House:

- › **Convene a series of summits—on education, health, transportation, medicine, and other issues**, with outside experts and relevant federal agencies—to discuss ways in which the environment for innovation can be enhanced in the United States.

The Commission also recommends that Congress and the Administration:

- › Substantially **increase federal investment** in basic technology and other research that fuels America's leadership in the tech sector.

The Commission's full report of findings and recommendations for the Administration, Congress, and American people can be found at [FutureofTechCommission.org](https://www.futureoftechcommission.org).

The Future of Tech Commission proposes the following key federal legislative and executive actions to safeguard consumers' and families' privacy and personal data, curb abusive conduct by online tech platforms, combat cyber threats, secure our democracy, and maintain America's leadership in technological and economic innovation.

Congress and the Administration should:

1. Enact a **comprehensive Federal Privacy Law** that:
 - **Requires companies to implement policies of data minimization** with respect to personal data collection and use—i.e., in general, restricting their collection and use of data to what they require to provide their services.
 - **Requires an “opt-in” standard** for personal data collection and strong use restrictions.
 - Ensures that it is **as easy to withdraw consent to the collection and use of personal data as it is to grant it.**
 - Requires internet companies to implement and display a **standardized privacy-protection label**, much like the standardized nutrition label on food products.
 - Bolsters **capacity for enforcement of privacy standards and laws**, including greater resources for personnel, investigation, and fining ability for the Federal Trade Commission (FTC).

2. Update and strengthen the **Children’s Privacy Law** to:
 - › **Prohibit collection of data from teens who are 16 and under**, increasing the age from the current 12 and under.
 - › **Ban behavioral advertising to children under age 16.**
 - › **Prohibit manipulative design** practices that push inappropriate content to children.
 - › Require online companies to conduct and publicly disclose a **“Children’s Impact Assessment”** before the launch of a major new service or product.
 - › Require companies to adhere to **“Duty of Care”** regulations to safeguard personal data in their possession.

3. **Reform transparency & algorithmic amplification practices that harm children, families, and our democracy:**
 - › **Require tech companies to disclose** their data collection practices, content moderation practices, and algorithmic use, including data sets that are collected and used for algorithmic amplification or targeting.
 - › **Require clear, concise, and readily understood** policies and processes for moderating content and appealing content decisions.
 - › **Prohibit any algorithmic process that discriminates unlawfully** as defined by federal law.
 - › **Remove Section 230 immunity for paid promotion/advertising** in order to help prevent consumer fraud, protect voting rights, and prohibit hate crimes and illegal discrimination in economic and civic opportunities.
 - › **Grant dual authority to the FTC and state attorneys general** to enforce reforms to Section 230 and other consumer protection or anti-discrimination rules.

4. Establish proactive Regional Cybersecurity Centers—consisting of both public and private actors across critical industries—to support real-time public/private coordination, rapid response, and prevention efforts against personal and industrial cyberattacks.

In addition to endorsing and advocating for the legislative agenda above, the executive branch should:

1. Establish a **White House Technology Coordinating Council**, led by a Senior Director and bipartisan Tech Policy Advisory Group, to develop a coordinated tech policy strategy for the nation.
 - › Given the importance of the tech sector to our society and economy, and the urgent need for policy reforms, a more prominent coordinating entity, helmed by senior White House leadership, is warranted.

Protecting Your Information, Your Privacy, and Our Democracy

Thanks to the internet, Americans have **much broader, more convenient access to information, education, news, opinions, health care, entertainment, and connections** with friends and family—expanding opportunities and changing expectations and lives.

Social media platforms can expand our sense of community and civic participation.

but...

Many apps and platforms **track information about us** throughout our day—often without our knowledge.

These apps **use that information to target us with products, opinions, brands, and political ideas.**

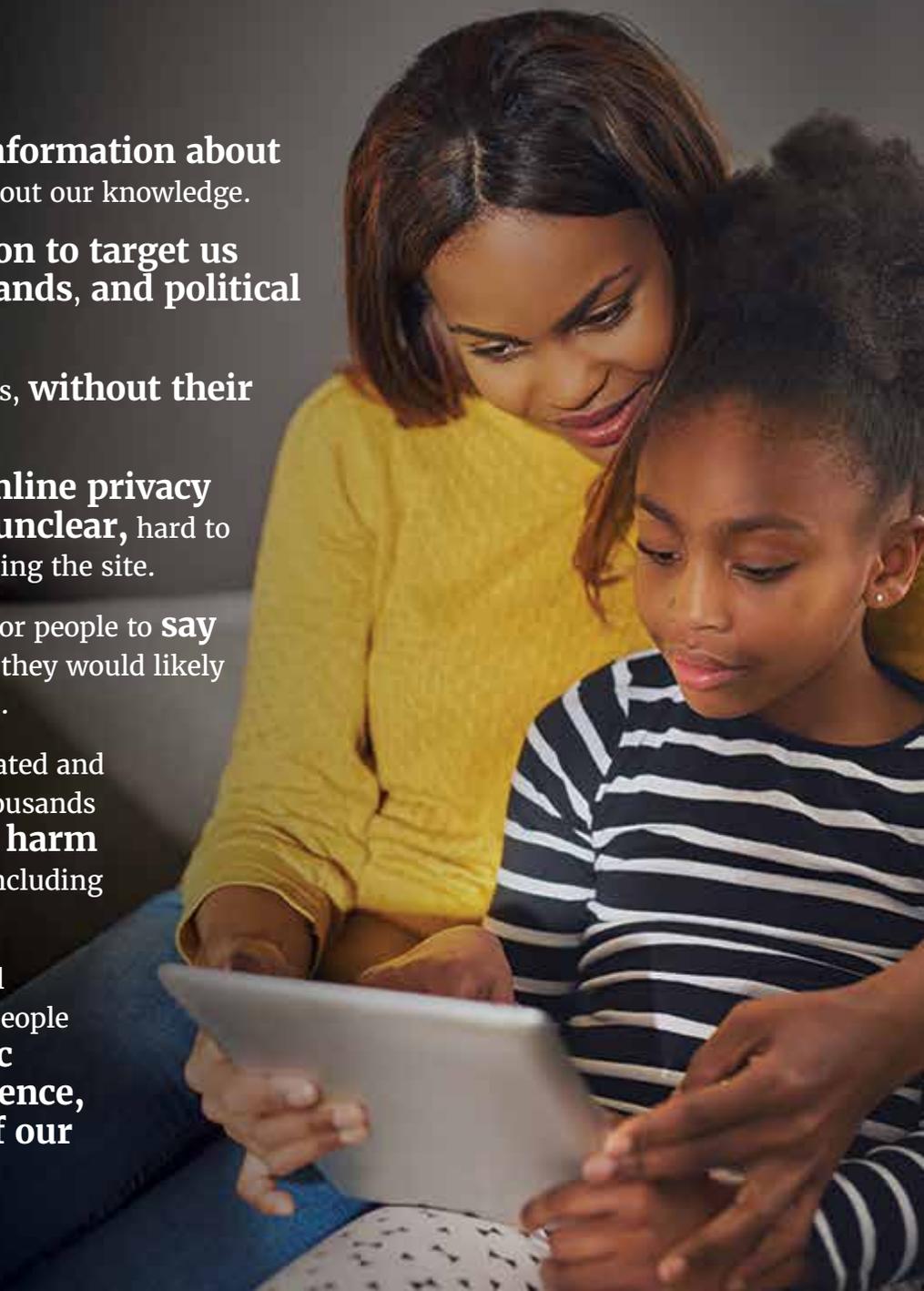
Some apps even track teens and kids, **without their parents' permission.**

Even **if we read and accept online privacy policies, many of them are unclear,** hard to understand, or an obstacle to accessing the site.

Social media can also make it easy for people to **say hurtful things to others** that they would likely never say to them when face to face.

When online harassment is coordinated and repeated at scale by hundreds or thousands of users, it can cause **real-world harm to individuals and groups,** including vulnerable kids and teenagers.

When illegal, harmful, or untruthful content is amplified to millions of people online, it can **undermine public health, promote offline violence, and threaten the stability of our democracy.**



The internet has created a world of good. Billions of people around the globe now enjoy extraordinary convenience, increased productivity, and immediate access to information, news, opinions, entertainment, and valued connections with family, friends, and wider communities of interest. The internet has profoundly changed lives, possibilities, expectations, and cultures, and extended America's leadership in innovation.

But like many advances, the internet also poses risks for users. Many of these risks we know little about, and some can threaten our safety, our economic security, our way of life, our institutions, and our democracy.

Protecting Your Privacy and Personal Information

When we use our smartphones or go online to check the weather, catch up on the news, or look up traffic conditions, for example, those sites and apps often collect sensitive personal information about us throughout the day. For instance, they can collect information about our habits, hobbies, geographic locations, interests, and friends. Many apps and websites then create sophisticated profiles about us that their advertisers use to target us with products, opinions, brands, or political ideas.

It's like being followed throughout the day, without our knowledge, by someone who is taking detailed notes about everything we do, everywhere we go, every website we visit, and how we interact with everything we encounter. Even children and teens are being tracked. Most people have no idea that their online data is being followed, collected, bundled, sold, and used—or misused—even if they read the privacy policies of the

sites they visit or the apps they utilize. Often, these policies are unclear or written in language that's hard to understand. Few, if any, are explicit about the reach, scope, and use of the data that websites and apps collect.

Many online sites collect personal information about us simply because they can, irrespective of whether that information is needed to provide a service to us. We heard in our town halls, for example, that some companies have collected billions of images and their tags from sites like LinkedIn, Facebook, and Instagram, and used artificial intelligence (AI) to instantly identify the people in them in any later photo or video, even if they haven't identified

Almost nine in ten voters—88 percent—agree that tech companies should be required to ask consumers whether they can use their data. And 80 percent agree that the federal government should do everything it can to curb the influence of big tech companies that use our data to reach too far into our lives.

“As a society, do we want to allow the sale of information about our children? Do we want to allow manipulation of older adults who don’t understand these practices?”

At some point we need to draw that line.”

—Ashkan Soltani, executive director of the California Privacy Protection Agency

themselves.⁵ This is especially alarming given that we don’t have a national standard for the collection of children’s images.⁶

No private company should have the latitude to collect, use, or disclose personal information about us without our explicit and informed consent. Americans deserve a safe, trustworthy internet they can use for convenience, information, innovation, communication, commerce, and community—without having their personal data harvested, bundled, sold, and misused. These online practices are a matter of national interest. According to a Washington Post–Schar School poll conducted in November 2021, 79 percent of Americans do not believe that tech companies provide enough control over how information about their activities is tracked and used. Our most recent nationwide poll, conducted in February 2022, reaffirmed these findings: 76 percent of Americans support restricting companies from collecting and using personal data beyond what’s needed for effective service.

We are especially concerned about the risks to teens and children. One study found that nearly 20 percent of apps specifically designated for children collect and share personally identifiable information about kids—data that can identify or be directly tied to them—without the knowledge and verifiable consent of their parents.

Indeed, as a general rule, tech companies collect, retain, and use far more personal information about users, including children, than they need for the services they offer. And we are not able to withdraw our consent as easily as we give it. In fact, many apps and websites condition our use of their services on our consent to their collection and use of our personal information. Even when we agree to allow apps to track and collect our data, tech companies often do not tell us exactly how our data is being used.

Curbing Abuse, Misinformation, and Harmful Amplification

Social media can also make it easy for people to say hurtful and destructive things to others that they would likely never say to them face to face, in real life. And when online harassment is coordinated and repeated at scale by hundreds or thousands of users, it can silence, stigmatize, and harm individuals and groups of people. Cyberbullying of vulnerable children and teenagers is cited repeatedly by parents, schoolteachers and leaders, and state-level policymakers as an example of this kind of hazard.

We personally abhor the lack of decorum and restraint so often in evidence online. But we have been careful not to impose our own views of what is or is not appropriate. Free expression is a public good in a democracy and must be safeguarded. Some social media platforms, including Reddit and Bumble, have explored different approaches to content moderation, and we note that most platforms have terms of service that ban abuse, harassment, and hateful conduct—which, as private companies, they are free to do. And yet tech companies have not been held accountable for their track record in enforcing these rules, or for investing sufficiently in the technology or personnel required to ensure compliance with their own policies.

Tech companies’ more serious and controversial online practice is called “amplification.” Many online platforms use algorithms—mathematical formulas that are rarely publicly disclosed—to decide what content to promote

⁵ Jonathan Zittrain, Harvard Town Hall.

⁶ Marc Ambinder, USC Town Hall.

and to whom. Algorithms are used to increase or decrease the visibility of certain content or to target individual users—for example, by recommending popular accounts or posts in a user’s news feed. Algorithms can highlight content that raises awareness of important civic issues, often from historically marginalized voices. They can promote posts and news stories that expose gender, racial, or other discrimination. Algorithms can also bring greater exposure to information about global issues, human rights violations, consumer complaints, corruption, or government malfeasance. During an emergency or natural disaster, algorithms can bring content to the attention of users that informs and even saves lives.

But algorithms can also have downside consequences, by amplifying inequalities and power imbalances. Some algorithms can lead platforms and advertisers to violate civil rights laws prohibiting discrimination in housing, employment, and credit based on users’ race, gender, and other classifications. According to a 2021 study, for example, Facebook’s ad platform continues to offer multiple ways for advertisers to discriminate by race and ethnicity, violating civil rights regulations.⁷

Significantly, some algorithms are designed to boost the visibility of content that sparks divisiveness, provocation, hatefulness, and outrage—because some tech companies rely on sensational content to attract and retain viewers. The larger the number of users, and the longer such users linger on the service, the more attractive the platform is to potential advertisers who are looking to buy ads on it. Senate testimony about Facebook in the fall of 2021 made clear that it is in the commercial interest of some platforms to amplify posts that fuel user engagement, even if the companies’ terms of service prohibit their content. As experts like Facebook whistleblower Frances Haugen have noted, Facebook, YouTube, and other social media platforms are aware that the amplification of sensational or provocative content by their algorithms is

central to their revenue strategy. In a very real sense, the more outrageous, divisive, and hateful the content, the better it is for their business.

The past several years have also seen a massive, sometimes malicious, assault on our sense of shared reality. The dissemination of falsehoods and conspiracy theories at scale on social media can cause real-world harm when amplified to millions of people.⁸ The amplification of health and political misinformation originates from a variety of sources. This content is corrosive to our safety, values, and civic life, and some of it is disinformation actively sponsored or disseminated by foreign state actors. Although much of that content is constitutionally protected, there are steps that policymakers and the private sector can take to safeguard our well-being, our civil rights and liberties, the fundamental norms of our democracy, and basic decency.

For example, content-neutral social media “circuit breakers”—like those used in the stock markets—could require online platforms to briefly pause the rapid amplification and dissemination of specific content that begins to go viral to an exceptional degree. Companies and policymakers would need to determine what “virality” trigger might be appropriate for discrete services with different attributes. But by hitting the “pause button” in key moments, platforms could determine, in real time, if such content violates their terms of service—enabling stepped-up, timely enforcement of their own corporate content policies or the law.

Greater transparency around companies’ use of algorithms is another important step. We should also strongly encourage all platforms to strictly enforce their terms of service and provide greater transparency around content mediation enforcement. These and other measures are available to private companies and organizations now and raise no federal, legal, or constitutional issues.

7 Jinyan Zang, “Solving the Problem of Racially Discriminatory Advertising on Facebook,” Brookings, Oct. 19, 2021, <https://www.brookings.edu/research/solving-the-problem-of-racially-discriminatory-advertising-on-facebook/>.

8 Foreign state actors employ a variety of tactics, including inauthentic or malicious accounts, to sow division and disseminate harm.

By contrast, government regulation of content raises important questions of free expression. We believe that free expression is a public good and have steered clear of proposals that Congress or the Administration legislate or regulate in the area of inappropriate or unpopular content. However, we do not believe that the government’s hands are completely tied.

While our Constitution guarantees freedom of speech, it does not guarantee freedom of reach.⁹ When illegal, harmful, or untruthful content is amplified to millions of people online, it can cause personal trauma, undermine public health, promote offline violence, and threaten the stability of democracy in the U.S. and around the globe. These are areas where Congress has already acknowledged a compelling public interest.

The privileges and constraints of the First Amendment mean that policymakers must find constitutionally sound ways to advance the public interest. While some of the content cited today as hurtful or harmful to public health, civic discourse, and our democracy is constitutionally protected speech, the real-world harms such content causes are enabled by the massive harvesting of our personal data and the use of that data—through algorithms—to target and provoke. Addressing these root causes in a direct, comprehensive way through a strong data protection and privacy law could yield healthier online public squares and valuable progress in our information ecosystem.

After years of unchecked growth, **82 percent of American voters now agree**, on a bipartisan basis, that we need to do more to regulate big tech.

For nearly half a century, the internet has remained largely unregulated. In that time, extraordinary innovation has spawned a powerful industry that has changed the world. Historically, Americans have created “rules of the road” to support investment and innovation while managing the risks of many life-changing innovations, from electricity to automobiles and airplanes. We believe it’s now in the national interest to put such rules in place for tech companies to protect our rights, safety, health, and families—to create sensible, effective guidelines for internet use that protect the privacy of individuals and children and put American consumers in charge.

⁹ Renee DiResta, “Free Speech Is Not the Same as Free Reach,” *Wired*, Aug. 30, 2018, <https://www.wired.com/story/free-speech-is-not-the-same-as-free-reach/>.

CONCLUSIONS AND RECOMMENDATIONS

To balance the importance of supporting an open society and a thriving, innovative economy with the urgency of protecting the freedom of expression and privacy of Americans, the Future of Tech Commission agreed to certain fundamental principles:

First, Americans deserve a safe, trustworthy internet that enables them to leverage its power for improved access, convenience, innovation, communication, productivity, commerce, and social good without having to sacrifice their privacy unknowingly or having their information harvested or used unreasonably;

Second, individuals should be able to control their own data, including knowledge of and agency over how it can be collected, utilized, shared, bundled, sold, or leveraged across platforms; and

Third, private enterprises and organizations should be required to abide by principles of data minimization and not collect more information than is necessary for their services or share, sell, or use such information about individual citizens or groups of citizens without explicit consent.

Accordingly, the Commission concludes that “opt-in” should be the standard for information gathering by tech companies—meaning that individuals must affirmatively give consent for the gathering, use, and sharing of personal information.

Further, it should be as easy to revoke consent as it is to grant it. And, to ensure that consumers have real bargaining power, it should be prohibited to condition the use of an app or website on the granting of consent to the collection of personal data not otherwise required to render service. The privacy of individual data must exist by default and design wherever possible, and data minimization is essential to addressing business models that fuel unsafe, unhealthy, manipulative, and anti-competitive behaviors.

Moreover, when users consent to having their data tracked or collected, companies must be clear about exactly what is being tracked and how it is being used. This includes when and how data is used in algorithms and algorithmic amplification.

Even with protective defaults, however, transparency and consumer education are needed to ensure companies' compliance with existing laws and meaningful control by individuals over their online experience. A digital citizenship agenda is essential to empowering consumers.

We also conclude that the privacy of kids and teens is paramount, and that solutions must ensure robust protections for children age 0–16. Parents must be empowered to play an active role in protecting their children's privacy. At the same time, the federal government, companies, and platforms all have a responsibility to ensure that the onus to protect a child's privacy does not fall entirely on parents.

The Commission acknowledges that many states have enacted or are considering online privacy laws or regulations. Some are models for our proposed federal actions. But rules that vary widely by state for online corporate behavior do not take practical account of the ubiquity of the internet itself, which operates without state boundaries. Since its impact on the public interest is national, indeed global, federal action is indispensable. Existing state laws are necessary but insufficient models; therefore, state laws should be considered the floor, not the ceiling, for federal action.

The federal government has an important role to play in bolstering those protections, especially for children, and in ensuring timely, robust compliance and enforcement.

Social media presents, perhaps, the greatest benefits and greatest hazards of the internet age. We are more connected to each other in a variety of ways, but we have also become more isolated from each other by the hatred, division, and discord spread and amplified on social media.

The concern about harmful online content quickly turns into a debate about freedom of expression under the First Amendment to the Constitution. Free expression is a sacred public good and must be fiercely safeguarded—even when such expression is hurtful, provocative, or unpopular. We recognize that rigorous protection of free expression sends a powerful signal to the rest of the world, especially to more closed or autocratic societies, and is another reason to tread lightly here. We do not believe that government can determine which content to regulate, except in limited circumstances. We therefore do not recommend federal legislation to regulate online content.

However, we do urge federal legislation and other enforcement actions that constrain the amplification of online content already deemed illegal—such as posts that directly incite imminent criminal activity or consist of specific threats of serious violence targeted against any person or group. This constraint can be done without placing an undue burden on free online expression, and it should be done promptly. Real-world harm can and has come from illegal or harmful content repeated at scale by algorithms. For this reason, we also recommend that the Department of Justice review federal criminal statutes to ensure that such laws are keeping abreast of technological and societal change.

We are mindful of the concerns of those who offer unpopular or dissenting ideas online. The natural, organic spread of such ideas should depend on their strength; that is precisely how unpopular views and dissenting opinions become mainstream in a free society. But when the ideas are spread by mathematical formula—and when the formula favors the most unfounded, sensational, or antisocial content—we conclude that social media platforms cross a line. In those circumstances, technology is no longer a tool for communication and connection, but rather an engine to drive division and public harm in service to profits of the corporation. And again, it is data that fuels that engine—our personal data.

In summary, the Commission concludes that federal leadership on privacy is needed to protect consumers and minimize harmful data practices. **We specifically recommend the following immediate actions.**

1. The Administration should propose and Congress should enact a comprehensive National Data Protection and Privacy Act that protects consumer privacy by placing strong national limits on the harvesting of private, personal data. At a minimum, new legislation should:

- Require an opt-in standard for personal data collection and use.
- Ensure that withdrawal of consent is as easy as granting it.
- Allow consumers to restrict the use of any personal data.
- Allow consumers to block any use, sharing, disclosure, or sale of their data with/by third parties.
- Beyond data strictly required to render service, prohibit companies from unfairly tying consumer consent of data collection and use to access of the product or service.
- Affirm that all federal laws and regulations prohibiting discrimination in the physical world apply to the amplification and impact of content in the digital world.
- Require companies to file regular transparency reports on data collection practices.
- Require platforms to produce a “data collection & use label,” like the standardized nutrition label on food products.
- Require companies to adopt “duty of care” regulations to safeguard personal data in their possession.¹⁰
- Update the Children’s Privacy Law to ensure adequate consumer protections for children.

¹⁰ Duty of care is the standard legal responsibility of an organization to avoid behaviors or omissions that could reasonably be foreseen to cause harm to others.

2. Congress should strengthen capacity for enforcement of privacy and dataprotection standards and laws. At a minimum, this should include:

- › Expressly authorizing the FTC to enforce the provisions of the new National Data Protection and Privacy Act.
- › Providing the FTC with greater latitude to fine violators, issue significant fines for first-time violations, and seek equitable relief.
- › Allocating more FTC resources for personnel to investigate and enforce privacy and data protection standards and laws.
- › Granting states' attorneys general concurrent jurisdiction to enforce the new federal privacy/data protection law, eliminating the need for a patchwork of state and local laws and rules.

3. To address issues raised by content moderation and amplification, the Administration should also propose and the Congress should also pass legislation that:

- › Affirms that all federal laws and regulations that prohibit discrimination in the physical world apply to the impact of content in the digital world.
- › Addresses algorithmic or other amplification of content already deemed illegal—such as posts that directly incite imminent criminal activity or consist of specific threats of serious violence targeted against any person or group.
- › Requires tech companies to disclose and be transparent about:
 - » Algorithmic use (and the data sets that are collected and used for algorithmic amplifications or targeting).
 - » Practices for moderating content, including but not limited to the mix of automated vs. human moderation, language coverage, and whether any users (e.g., VIPs) are treated differently than ordinary consumers and, if so, how.

- › Removes Section 230 immunity for paid promotion/advertising in order to help prevent consumer fraud, protect voting rights, and prohibit illegal hate crimes and discrimination in economic and civic opportunities.
- › Considers the removal of Section 230 immunity for product design features to ensure that the results of product design mechanisms—such as recommendation algorithms and video content suggestions—are not treated as user speech for purposes of Section 230, to the extent to which the results (i.e., the recommendations) cause harm. Because these design tools are closely tied to free expression, Congress should tread carefully in this area to avoid unintended consequences.¹¹
- › Expressly grants authority to the FTC to enforce Section 230, as reformed, with respect to removing immunity for paid promotion/advertising, and including significant power to fine.
- › Requires online platforms to have clear, concise, and readily understood policies and processes for moderating content. People who use these services should have the right to clear rules, transparent enforcement, and equitable and timely appeals.
- › Affirms that it is unlawful for an online company to employ any algorithmic process that discriminates in or otherwise makes unavailable the goods, services, facilities, privileges, advantages, rights or opportunities, or accommodations of any place of public accommodation on the basis of a user's or class of persons' actual or perceived race, color, ethnicity, religion, national origin, age, sex, gender, gender identity, sexual orientation, or disability.

4. Regulatory agencies and departments should leverage their existing authorities to protect against algorithmic discrimination as follows:

- › The FTC should utilize existing authority (such as section 5 of the FTC Act, the Children's Online Privacy Protection Act (COPPA), and the Equal Credit Opportunity Act) to police and enforce violations of these laws and illegal, discriminatory algorithmic results.

¹¹ An example of a current deficiency in the law is the case of *Herrick v. Grindr*, in which product design mechanisms enabled a bad-faith user to impersonate and abuse an ex-partner.

- › Other federal departments and agencies should similarly identify the legal authority they may already possess to address violations of existing law in the online space.
- › The Department of Justice should review federal criminal statutes to ensure that such laws are keeping pace with changes in society and technology with respect to online content and recommend to Congress any legislative changes such review identifies.

5. In addition, Congress should give the FTC authority to:

- › Reclaim lost consumer dollars in 13(b) cases. (Swindlers should not be able to retain ill-gotten gains from Americans.)
- › Impose initial fines for first-time violations of FTC rules and the power to enforce this.
- › Require large online companies to disclose to the agency and the general public the nature of algorithmic use in online services.
- › Require large online companies to share data with researchers for academic inquiry, stipulating the categories or content and the types of data that companies must make available.
- › Require online companies to conduct a “Safety Impact Analysis” before the launch of any major new service or new functionality, including a “Children’s Impact Assessment” for any service for which minors age 16 and under are likely to be a significant segment of the audience. The FTC should also be granted the authority to solicit a safety impact analysis upon request for any individual service. This analysis should be updated every five years.¹²

6. Platforms and services should be encouraged to:

- › Experiment with content-neutral innovations and implement effective tools to minimize harmful amplification and virality, such as “circuit

breakers” that constrict virality in times of highly spiked traffic.

- › Join and adhere to voluntary international codes of conduct, such as the Christchurch Call—a commitment by governments and tech companies to eliminate terrorist and violent extremist content online—and participate in collaborations such as the Global Internet Forum to Counter Terrorism (GIFCT).

The Commission received a wide variety of other meritorious ideas through our outreach. We find the following to be the most compelling and urge further consideration of them by the Administration and Congress:

1. To address the impact of online platforms on the deterioration of local newsreporting and outlets:

- › Enhance Corporation for Public Broadcasting support for local news gathering and dissemination of civic information content, especially in rural areas.
- › Create a Public Interest Media Fund to invest in trusted local sources of information, supported in a public-private partnership by financial contributions or taxes on tech companies, a percentage of money from FTC fines, and/or a merger transaction fee.
- › Encourage the development of independent, nonprofit local news centers to elevate the voices of citizens in communities where journalism resources have diminished in recent decades.

2. Support media literacy and digital citizenship programs that foster digital integrity for families, children, and the elderly to combat misinformation and protect democracy.

¹² Similarly, Australia’s “Safety by Design” approach encourages technology companies to alter their design ethos from “moving fast and breaking things” or “profit at all costs” to moving thoughtfully, investing in risk mitigation, and embedding user protections at the front end. <https://www.esafety.gov.au/industry/safety-by-design>.

Hardening America's Cybersecurity

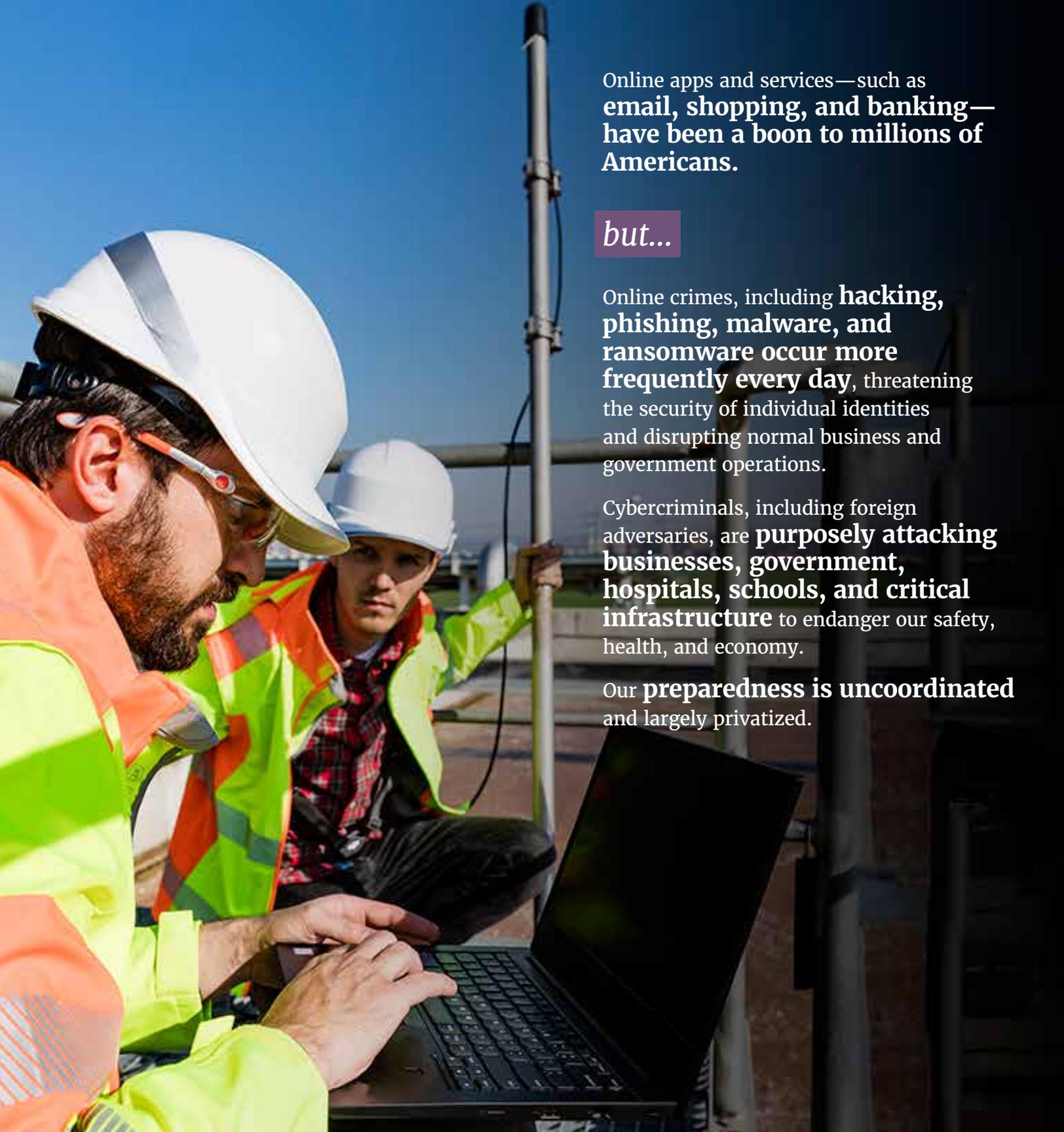
Online apps and services—such as **email, shopping, and banking**—have been a boon to millions of Americans.

but...

Online crimes, including **hacking, phishing, malware, and ransomware** occur more frequently every day, threatening the security of individual identities and disrupting normal business and government operations.

Cybercriminals, including foreign adversaries, are **purposely attacking businesses, government, hospitals, schools, and critical infrastructure** to endanger our safety, health, and economy.

Our **preparedness is uncoordinated** and largely privatized.



Millions of Americans enjoy the conveniences of email, online shopping, internet banking, and other web-based services. Many of us apply for public benefits, utility services, insurance, or healthcare online. We disclose confidential personal and financial information to gain access to those services or complete transactions. Even when consumers shop, bank, or sign up for a phone service in person, the credit, debit, or identification card we swipe captures our information, then processes and stores it in online systems.

The companies, utilities, and other organizations that collect and store that information recognize its value. So do cybercriminals, who may be individuals, domestic or foreign; criminal organizations; and sometimes even state adversaries. They hack customer databases. They launch phishing scams that use fake emails to steal credit card and Social Security numbers. They steal individual identities. They infect computer systems with malicious viruses to disrupt and disable pipelines or transportation services. Indeed, the tools and tactics they use to infiltrate legitimate data management systems are among the most inventive aspects of online life today.

The impact of cybercrime is significant. Identity theft has led consumers to experience profound disruption in their credit histories and benefit plans, and the attacks are constant. According to the FBI, cyberattacks have increased by 300 percent since the start of the COVID-19 pandemic, when Google was blocking more than 18 million coronavirus phishing attempts a day.¹³ In the 2020 SolarWinds cyberespionage attack, hackers thought to

be supported by the Russian government breached the data of as many as 18,000 private- and public-sector organizations, including U.S. government agencies, federal courts, state and local governments, and private-sector companies. About every 11 seconds, cybercriminals launch ransomware attacks, deploying software that holds computer systems hostage for ransom money. The average cost of a ransomware attack on the businesses they prey on was \$133,000 by 2021.¹⁴ These attacks can be devastating to American families, small businesses, industry, critical infrastructure, and even our hospitals and schools. Every month, according to the Treasury Department, cyberattacks cost American companies \$102 million in ransomware payments. "It's a tsunami," says former New York County District Attorney Cyrus Vance Jr., "and we have not yet embraced that reality as a country."

Many public and private sector leaders have taken steps to prevent cybercrime and strengthen cyber defenses, such as incident reporting; sharing of resources, training, and information among federal, state, and local agencies

13 Cobalt Labs, "Cybersecurity Statistics for 2021," <https://cobalt.io/blog/cybersecurity-statistics-2021>.

14 PurpleSec, "2021 Cybersecurity Statistics," <https://purplesec.us/resources/cyber-security-statistics>.

“Every time somebody digitizes all of the HVAC air conditioning, light, electricity in their building and moves away from a mechanical approach, they’re creating yet another opportunity for someone to find their way into somebody’s building, into their systems, literally into the guts of whatever their particular information and financial interest might be. **It’s now a nation-state game, and it’s incredibly well-financed.”**

— Governor Charlie Baker of Massachusetts

and between government and industry; and hardening our critical infrastructure. But these are not the norm, and such efforts are often hampered by jurisdictional limitations, lack of clarity, or competition. America also trails other countries in developing a highly trained cybersecurity workforce that is fully prepared to engage in this important work.

Isolated responses to existing threats or recent attacks are not sufficient to meet a growing, often well-planned and coordinated threat. America must take preventive measures to secure our tech infrastructure or risk fundamentally endangering our society and economy through the use of the very tech resources on which we have come to rely. Such measures must address the need for increased transparency of the scope and scale of attacks in the public and private sectors; improved coordination and deployment of federal resources; improved threat assessment and training across impacted organizations; coordinated responses to incidents involving foreign actors; and maintenance of sensitive information.

Cyberthreats can be national in scope, but many are hyper-local. In March 2021 alone, for example, 13 school systems and 17 hospitals, healthcare systems, and clinics disclosed ransomware attacks.¹⁵ We must, therefore, provide the necessary resources, expertise, and authority to enable federal, state, and local entities and businesses to harden their tech infrastructure through coordination and transparency. Covering those costs is a shared responsibility among all levels of government and the private sector.

¹⁵ Adam Janofsky, “Ransomware Tracker: Schools, Hospitals Face a Surge in Attacks,” *The Record*, April 17, 2021, <https://therecord.media/schools-hospitals-face-a-surge-in-ransomware-attacks/>.

Standards for how best to harden the security of a given technology or infrastructure will vary across diverse sectors. Law enforcement, for example, may have different needs and expectations than a military base, a commercial enterprise, a school system, or a college. The federal government may have responsibility to protect military bases, for example, but should nonetheless convene, empower, and resource local partners, such as local law enforcement, to develop incident responses and prevention strategies. Jurisdictional differences should not obstruct action or deter the sharing of information and experience. Transparency and coordinated action must be paramount.

Voters, on a bipartisan basis, overwhelmingly worry about our nation’s cybersecurity;

88 percent agree that one of the biggest threats is a data breach by foreign adversaries, and 81 percent believe that the country’s critical infrastructure will probably be hacked by an adversary in the next five years.

CONCLUSIONS AND RECOMMENDATIONS

Congress should act swiftly to pass strong national privacy laws that safeguard Americans' personal data, as proposed above, so that there is less personal information at large on the internet. Beyond that, experts repeatedly advised us that America's readiness to prevent and respond to cyberattacks depends on two fundamentals: transparency and coordination. Our recommendations in this area center on these key themes.

Accordingly, the Commission recommends that Congress enact cybersecurity legislation that promotes coordination and transparency among and across sectors; improves incident reporting to enable better response and preparation; and develops a workforce to support America's cybersecurity. Specifically, cybersecurity legislation should:

1. Create regional centers—including those focused on supporting rural communities—consisting of both public and private actors across critical industries (including transportation, healthcare, finance, telecommunications, public utilities, energy, emergency services, hospitality, media, tech, government, FEMA, education, and others based on local need). The mission of these centers would be to:
 - Share real-time threat and incident information (see below), including ransomware demands, between and among governments and the private sector.
 - Coordinate responses.
 - Train and share talent resources.
 - Develop and implement standards of preparedness by industry and best practices for coordinated responses, including minimum security requirements for software, hardware, and other technology procured using federal funds.
 - Disseminate tools to inform the general public—such as standardized “seals of approval” or a rating system—to help families and individuals better protect themselves.
2. Require that Cyber Incident Reports be provided to the regional center, in real time, regarding all material cyberattacks, data breaches, or credible threats experienced by or known to federal agencies and contractors; critical infrastructure operators; digital security firms; state, local, and Tribal governments; and private-sector companies.
3. Direct DHS to work with sector-specific risk management agencies to provide guidance, by industry, to relevant regulatory authorities, including the Federal Energy Regulatory Commission, the Federal Communications Commission, and the Department of Justice.
4. Appropriate funds to recruit and train a best-in-world cyber workforce through educational programming in community colleges, other higher education institutions, centers of workforce training, and K-12 classrooms.

Ensuring Open and Competitive Markets

Thanks to passage of the 2021 bipartisan Infrastructure Investment and Jobs Act, **universal access to reliable, high-speed broadband** is now achievable.

Large internet platforms and providers may **offer better services and be more competitive** in the global marketplace.

but...

Broadband grant administrators rely on **incomplete, outdated maps** of broadband service.

Obstacles to **availability and affordability** remain.

Internet **giants, meanwhile, can stifle smaller, innovative competitors** by acquiring them or copying their products.

Large platforms give consumers **limited power, choice, and control** over the content they see, create, and share across different platforms.



The Commission considered the impact on consumers of two kinds of market concentration: that of broadband providers and that of internet platforms.

Broadband Providers

As we concluded at the outset, high-speed, reliable broadband is essential today for every American everywhere. The 2021 bipartisan Infrastructure Investment and Jobs Act will now fund access for the more than 100 million Americans who lack it. The Act alone, however, does not directly address two remaining barriers that consumers face: adequacy and affordability.

Americans who live in areas with only one or two broadband providers pay prices that can be considerably higher than those who live in markets with more competition. According to a July 2021 survey by Consumer Reports, the median cost of broadband service was \$75 per month for Americans who said they had only one broadband service provider available to choose from, while broadband users who had four or more options paid a median of \$67 per month. In addition, 32 percent of Americans said that affordability was the reason they

A strong bipartisan majority of American voters—83 percent—support enacting regulations that enable a competitive, affordable broadband market.

did not have broadband.¹⁶ In Wisconsin, for example, 40 to 60 percent of households earning less than \$20,000 in areas that had broadband service still lacked internet access, compared to 5 percent to 15 percent of households earning more than \$75,000.¹⁷

Encouraging competition from companies that offer an array of broadband technologies—from cable and fiber to satellite and wireless, so long as they meet minimum needs for speed and reliability—can help improve service quality and affordability in communities that have broadband and accelerate delivery of service to communities without it, with the implementation of the Infrastructure Investment and Jobs Act’s new resources for broadband expansion. Another promising trend is the increasing number of rural cooperatives and municipal utilities providing broadband connectivity to unserved households.

“Access is not meaningful if it’s not affordable.”

— Chet Kanojia, co-founder of Starry, Inc.

¹⁶ Consumer Reports, “Broadband Survey,” July 2021, https://advocacy.consumerreports.org/wp-content/uploads/2021/08/CR_Broadband-Survey_8_2021_VF.pdf.

¹⁷ Jackson Parr, Tessa Conroy, Steven Deller, and Matt Kures, “Broadband Access and Affordability,” <https://economicdevelopment.extension.wisc.edu/2021/06/08/broadband-access-and-affordability/>.

Internet Platforms

Meanwhile, online platforms have become a huge part of life for most Americans, and digital giants—including Apple, Amazon, Google, and Facebook—own a very large share of the marketplace. Such scale may offer benefits to consumers. Search engine platforms, for example, can perform better and more efficiently at large scale, because their costs can be lower to provide instant, high-quality search results with the greatest depth of information. Depending on how they organize and present the information they have (see our recommendations on data privacy above), large tech companies may advance the position of the U.S. as the world’s most democratic innovator.

At the same time, scale may impede competition, especially from small businesses. Consumers have little power over the personal information they provide and the content that platforms make available to them. Internet giants can and have crowded out small, innovative competitors by favoring their own products on their platforms, acquiring competitors, or copying other companies’ products or services to achieve vertical integration—creating their own proprietary pipelines of suppliers, distributors, and sales outlets in online ecosystems. AI interoperability is another challenge. Although you can use your cell phone to call family, friends, and coworkers no matter what carriers they use, you can’t share your information and posts among different, competing platforms. They operate, in a sense, like walled gardens that keep online users inside.

In addition, consumers cannot transfer their content from one social media platform to another. Mobile phone

“Fostering global business growth and protecting customers are not mutually exclusive. We must prioritize both.”

— Enrique Lores, president and CEO of HP Inc.

customers, for example, can often retain their existing phone numbers and contacts when they switch from one competing carrier to another. But when consumers decide to leave one social media platform and use a different one, they don’t have the option of transferring their posts and contacts.

Our process led to a consensus that America deserves a market for internet technology and services that is second to none. We need a market that is conducive to investment and innovation, job creation, and entrepreneurial entry. The Department of Justice, Federal Trade Commission, and several state attorneys general are actively engaged in antitrust investigations, litigation, or other enforcement action in this area. We are sensitive to involving ourselves directly in such ongoing actions and inquiries.

The Commission does believe, however, that the U.S. is stronger and the marketplace healthier when markets are open, fair, inclusive, and fully competitive. At the same time, we also acknowledge the global supremacy and scale of American innovation. We believe such markets serve the needs of consumers, small businesses, and entrepreneurs and foster our international competitiveness in a fiercely competitive global economy. We acknowledge, however, that America’s large tech companies and platforms have a disproportionate share of the market and outsized market power. We are concerned about their vertical and lateral growth and the impact of excessive market power on consumers, small businesses, and competitors. Accordingly, the Commission recommends and supports efforts in Congress and the Administration to enforce our nation’s competition laws and reinforce our commitment to fair and open markets by strengthening the tools of regulators and antitrust enforcers.

A majority of voters, on a bipartisan basis, agree that a handful of very large companies dominate the sector, making it **very difficult for new companies or startups to compete.**

CONCLUSIONS AND RECOMMENDATIONS

The Commission concludes that the future of technology in Americans' lives must include free and fair competition. We agree with history and the many experts we consulted that greater innovation, lower prices, and broader consumer choice are all enhanced by competitive forces in the private market. Part of ensuring this will require that administrations use the authority they have under existing laws and regulations to review mergers and acquisitions, with adequate resources to do so. We note that President Biden's Executive Order issued in July 2021 has initiated a review of this.

The Commission also concludes that consumers must have opportunities and the ability to use their personal information across platforms. To enable this competition, critical services must be unbundled to allow consumers to leverage different platforms, tools, and technologies.

Enhanced competition goes hand in hand with data minimization and privacy—ensuring that the overwhelming amounts of personal data collected by a few large actors do not stifle new entrants to the marketplace.

To ensure against anti-competitive or unfair business practices that harm consumers, the Commission recommends both executive and legislative action. Specifically, the Commission recommends that the Administration direct the DOJ and/or the FTC, as appropriate, to:

1. **Enhance scrutiny of tech mergers and acquisitions to specifically determine what benefits of cost, choice, and security are served to consumers.**
2. **Improve coordination with state attorneys general of oversight of anti-competitive behavior.**

3. **Increase coordination with international antitrust enforcement agencies—specifically, collaboration with foreign democracies around enforcement remedies.**
4. **Supplement FTC and DOJ budgets to ensure thorough and timely investigations and enforcement with respect to merger and acquisition activity in the tech industry.**

The Commission also recommends that Congress enact legislation to foster improved competition, **greater innovation, and more consumer choice** by requiring that online platforms provide consumers with:

- Data portability—allowing people using social media platforms to port their personal data and content, as applicable, to other platforms.
- Interoperability and cross-posting—allowing people using major social media platforms to cross-post content onto other online platforms and vice versa.
- Access to “middleware” technologies and services—software that connects two or more different platforms or applications, enabling communication between them and new functionalities—enhancing competition and consumer choice.
- Algorithmic choice and open social media protocols to create an array of new options for people to have a personalized, fair, and level playing field of experiences.

Sustaining America's Leadership in Innovation

America has been the **world's technology leader** for decades.

Investment by the federal government in **basic scientific research spawned the technology revolution**, including the internet, GPS, smart-phones, search engines, and other breakthroughs.

but...

U.S. investment in basic research has dropped significantly since the 1960s.

China now manufactures most U.S. tech products, threatening our supply chain, and invests heavily in new technologies, such as artificial intelligence, which could have a profound impact on our lives.

Other countries now lead in the development of tech policies and practices that protect consumers and fair competition.



For more than 30 years, the U.S. has been a global tech leader—developing world-class online products and services, creating industries and millions of jobs, and improving convenience and productivity. As more and more of our transactions and interactions occur over the internet, however, attention is shifting to policies and practices that protect consumers and marketplace competition online. Other governments are well ahead of the United States in formulating and implementing such policies. Indeed, leaders of our own tech sector now call for us to develop coordinated tech policies that safeguard privacy, defend open markets, and enhance our access to critical supply chains—or else we risk squandering the leadership we've had.

Roughly 120 countries, for example, have already passed national privacy laws. The United States has not—a factor that can erode confidence in American products and make it challenging for U.S. companies to comply with a global patchwork of regulations. Europe, in particular, has been a leader in legislating tech practices. There is now strong agreement among voters and tech industry leaders that the U.S. needs a strong national privacy law to protect consumers, as proposed above. Sustaining America's tech leadership is yet another reason to do so.

The U.S. is also losing control of its supply chain to China. China now makes most of the tech products sold by American firms. China's dominance in tech manufacturing is a function of decisions that American companies have made, over time, to offshore manufacturing to places where costs of labor, housing, and doing business are cheaper. This has resulted in favorable short-term costs for American companies and arguably lower prices for consumers, but it has also placed our supply chains, and in some cases our intellectual property, at risk over the long term.

“There's a big geopolitical reason for aligning with Europe on national privacy laws. We have a model to look at and a transatlantic dialogue to engage in that can help us see ways forward.”

— Daphne Keller, director, Program on Platform Regulation, Stanford Cyber Policy Center

“We used to sell 40 percent of the semiconductors around the world, but now nearly 80 percent of semiconductors are produced in Southeast Asia.

We need to create federal incentives to help attract and retain semiconductor manufacturing capabilities here in the United States.”

— Arizona Senator Mark Kelly (D-AZ)

At the same time, the Chinese state has invested deeply in materials and new technology, notably artificial intelligence (AI) and quantum computing, that many tech leaders believe will be the platform for future transformative innovation and growth. It would be impossible for an individual American company to invest in the basic research that underlies these and other cutting-edge technologies at the level of the government of China.

The United States has a powerful history of technological innovation. Most tech companies today benefit from the government’s foundational investment in basic scientific research through the 1950s and ’60s. That taxpayer investment spawned the internet, global positioning satellites, search engines, smartphones, supercomputers, MRIs, the human genome project, and countless other breakthroughs. It attracted the best scientists across the globe to the United States to innovate, and led to a technological revolution that changed the world. It is a proven model.

Since 1964, however, federal investment in research and development (R&D) has dropped from 2.5 percent of GDP to 0.6 percent. Since 2011 alone, U.S. government investment

in R&D dropped by 12 percent, while China’s research investment jumped 56 percent.

Although American innovation has benefited from private-sector R&D investment—which climbed from 0.7 percent of GDP in 1956 to 2.0 percent in 2014—most of that investment has been used for product development, building off of ideas developed through government-funded research. Only 20 percent of private-sector R&D has supported basic scientific research, the engine of our innovation economy.

Nine in ten American voters agree that technological innovation will transform the way Americans live, work, learn, and connect with each other.

Similarly, we have been slow to invest systematically in building a well-educated and digitally literate workforce. There are examples of functioning private-public partnerships, but the scale of investment may not be sufficient to meet the competitive need.

America should continue to lead the world with the best technologies and talent. Today, new technologies such as AI and quantum computing—which could speed the processing of complex information and perform computing tasks that are now impossible—are poised to change such fundamentals as the nature of work and national security. The private sector cannot and will not address those interests entirely on its own.

“If the U.S. doesn’t exercise more leadership in tech policy, **it’s ceding leadership to other countries.**”

— Brad Smith, president and vice-chairman of Microsoft

CONCLUSIONS AND RECOMMENDATIONS

Many democratic allies around the world are taking action to bolster privacy protections and hold companies and institutions accountable to the public. The Commission believes there is a national interest in joining them to protect our own interests, values, and opportunities. We believe that American tech innovation leadership depends on it.

We also conclude that the United States has an interest in rising to meet the challenge of China’s technological development and influence, that a coordinated tech approach is essential to doing so, and that policy coordination will support strategic technological innovations, open markets, and the values of safety, human rights, and free expression.

A well-educated and digitally literate workforce—prepared to safely and effectively leverage technology to catalyze local innovation and spur community economic development—must also be an essential feature of American tech leadership. Government has a role to play in supporting the development of such a critical workforce.

Some of the foregoing will suggest certain approaches in foreign policy. For example, the Commission urges the Administration to recognize the leadership that other governments—such as the EU, Australia, Ireland, Canada, and the UK—are providing in formulating policies that are consistent with democratic values. The Administration can engage immediately on global policy alignment through the U.S.-EU Trade and Technology Council, the G7, and other international fora. At the same time, a Technology Coordinating Council in the White House can help advance American global leadership in internet policy, technology, and innovation.

The White House should also convene a summit of tech leaders and others to discuss the contours of policy coordination, the nature of supply chain constraints and opportunities, and the scale of needed public investment in basic research.

In addition, the Administration should:

1. **Create a Technology Coordinating Council in the White House to coordinate and drive policy impact, consistent with President Biden’s Executive Order of July 9, 2021, the recommendations of this report, and other strategic global and domestic technology goals.**
2. **Increase federal investment to support technology research through the National Science Foundation, the National Institutes of Health, and the Department of Energy’s Office of Science and its 17 national labs.**
3. **Fund research initiatives, competitions, and collaborations across these and other agencies that focus on cybersecurity, privacy, AI, and cloud computing.**
4. **Leverage technological tools to develop a personal security emergency alert system, similar to FEMA’s Integrated Public Alert & Warning System.**
5. **Prepay for enhanced quantum computing technologies through a public-private partnership wherein significant support (approximately \$500 million per year) is allocated to the country’s top three to five quantum computer development projects.**
6. **Reinforce and safeguard artificial intelligence markets in conjunction with the National AI Research Task Force, advocating specifically for:**
 - The authorization of an independent, federal Artificial Intelligence Board within the FTC, which can, among other things, designate official risk categories for AI systems, each with proportionate risk-based legal regulations and codes of conduct.

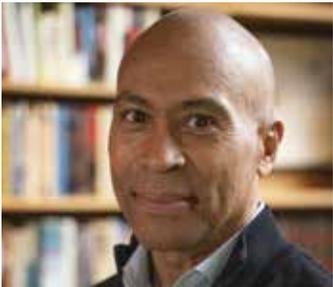
- › The creation of a comprehensive national database of AI system records and processes, particularly for those stand-alone high-risk systems with fundamental human rights implications. The database could provide graduated access levels to regulators, researchers, and the public while giving regulating entities the ability to audit and accredit AI companies.
 - › The support of regulatory sandboxes and innovation hubs wherein companies can develop safe, ethical AI systems.
7. Enhance the United States Digital Service and 18F (<https://18f.gsa.gov>) to bolster pipelines of technology talent into public service and support improvements in government service delivery. In addition to these federal programs, this model could support grants for state and local programs to bolster their recruitment and retention of government talent in leveraging technology to improve government function.
8. Develop a new “Digital Inclusion Fund” at NTIA to address digital divide concerns and support subscriber acquisition for new entrants. Also include:
- › A program for institutions working to bridge the digital divide in local communities (e.g., schools, libraries, public housing, health clinics), including leveraging digital navigators.
 - › Funding for digital needs assessments, digital citizenship/skills programs, bulk purchasing of home broadband service, and bulk purchasing of devices.

FUTURE OF TECH COMMISSIONERS



Margaret Spellings

Margaret Spellings is president and CEO of Texas 2036, a long-term, data-driven organization working to secure Texas' prosperity through the state's bicentennial. Her extensive leadership in education and government includes serving as president of the University of North Carolina System and president of the George W. Bush Presidential Center, as well as U.S. secretary of education and White House chief domestic policy advisor for President George W. Bush.



Deval L. Patrick

Deval L. Patrick is a business and civil rights attorney, a former senior executive in two Fortune 50 companies, an impact investing entrepreneur, and the former two-term governor of Massachusetts. He is the author of two books, *A Reason to Believe: Lessons from an Improbable Life* and *Faith in the Dream: A Call to the Nation to Reclaim American Values*, a devoted spouse of 36 years to Diane, a lover of Labs, and a beekeeper.



James P. Steyer

James Steyer is the founder and CEO of Common Sense, the nation's leading independent nonprofit organization dedicated to creating a powerful voice for kids and families in the 21st century. He is also the author of his latest book, *Which Side of History: How Technology Is Reshaping Democracy and Our Lives* (2020), an award-winning consulting professor at Stanford University, and the dad of four great kids.

TOWN HALL LOCATIONS & PARTNERS

The Commission partnered with leading civic organizations and academic institutions to convene nine town halls across the country and two in Europe. More than 1,000 local attendees joined those discussions.

Arizona (Arizona State University)

A Public Discussion on Digital Equity, Access, and Tech Innovation for Workforce

California, Northern (Stanford Cyber Policy Center)

A Public Discussion on Creating Safe, Healthy Online Spaces for All Americans

California, Southern (USC Annenberg School of Communication and Journalism)

A Public Discussion on Creating Safe, Healthy Online Spaces for All Americans

Connecticut (Office of the Governor, Connecticut Commission for Educational Technology, and Connecticut State Department of Education)

A Public Discussion on Advancing Innovations in Education

Florida (Knight Foundation, with ExcelinEd and Florida Chamber of Commerce)

A Public Discussion on Advancing Innovations in Tech Education and Talent Development

Indiana (Purdue University)

A Public Discussion on Digital Access and Workforce Development in Rural and Agricultural Communities

Massachusetts (Harvard Kennedy School)

A Public Discussion on Creating Safe, Healthy Online Spaces for All Americans

North Carolina (Duke Health and UNC Health)

A Public Discussion on Leveraging Technology to Accelerate Innovation in Health Systems

Texas (Texas 2036, University of Houston)

A Public Discussion on Digital Access for All, and Proliferating Technological Innovation in Education and Workforce

European Union (Tech Ambassador, Denmark)

United Kingdom (Carnegie UK Trust)

INTERVIEW & TOWN HALL PARTICIPANTS

Through interviews and town hall discussions, the Commission gathered input from approximately 150 experts, advocates, and industry and thought leaders, including:

Lisa Abbott, Executive Vice President for Economic and Community Development, Regional Opportunity Initiatives Inc.

Prabhat Agarwal, Head of Unit, Digital Services and Platforms, DG Connect

Robert Alvarado, VP, Information Management & Technology Services, Chicanos Por La Causa

Marc Ambinder, Adjunct Professor & Creator, USC Annenberg Center Digital Security Initiative

Nicole Anderson, President, AT&T Foundation & Assistant Vice President of Corporate Social Responsibility

Lorena Austin, Student, Arizona State University

Governor Charlie Baker, Massachusetts (R-MA)

Willow Bay, Dean, USC Annenberg Center

Larry Berger, CEO, Amplify

Senator Richard Blumenthal (D-CT)

Bryan Brayboy, Senior Advisor to the President & Director, Center for Indian Education, Arizona State University

David Brody, Senior Counsel & Senior Fellow for Privacy and Technology, Lawyers' Committee for Civil Rights Under Law

Dr. Wesley Burks, CEO of UNC Health Care, Dean of the UNC School of Medicine

Jeb Bush, Former Governor, Florida (R-FL)

Shawn Carpenter, Department Head, Information Technology, Ella T. Grasso Technical High School

Erin Carr-Jordan, PhD, Senior Director, ASU ADVANCE

Doug Casey, Executive Director, Connecticut Commission for Educational Technology

Ricardo Castanheira, Counselor Coordinator of Digital & Telecommunications, Portuguese Presidency of the EU

Dr. Stephanie Cawthon, Professor of Educational Psychology, University of Texas

Michael Conner, Superintendent, Middletown Public Schools, Connecticut

Tim Cook, CEO, Apple

Governor Roy Cooper, North Carolina (D-NC)

Jonathan Costa, Assistant Executive Director, EdAdvance

Geoffrey Cowan, University Professor & Annenberg Family Chair in Communication Leadership, USC Annenberg Center

Matt Crouch, Deputy Director, Indiana Office of Community & Rural Affairs

Melanie Dawes, Chief Executive, OfCom

Alberto Di Felice, Director for Infrastructure, Privacy & Security, Digital Europe

Renee DiResta, Technical Research Manager, Stanford Internet Observatory

Dr. Joan Donovan, Research Director, Shorenstein Center on Media, Politics, and Public Policy, Harvard Kennedy School

Andrew Ferguson, Chief Education Officer, Dalio Foundation

Dr. Jeffrey Ferranti, CIO and Vice President for Medical Informatics, Duke University Health System

Dr. Lynne Fiscus, President & CEO, UNC Physicians Network

Roberto Gallardo, Director, Center for Regional Development & Purdue Extension Community, Purdue University

Lev Gonick, CIO, Arizona State University

Julie Inman Grant, eSafety Commissioner, Australia

Jonathan Greenblatt, CEO, Anti-Defamation League

Angela Gunder, Vice President of Learning and Chief Academic Officer, Online Learning Consortium

Mary Haddad, Student, Arizona State University

Jaffus Hardrick, President, Florida Memorial University

Reed Hastings, Co-Founder and Co-CEO, Netflix

Frances Haugen, Facebook Whistleblower

Marcell Haywood, Founder and CEO, Encompass

Maura Healey, Attorney General, State of Massachusetts (D-MA)

Stephen Hegedus, Dean, College of Education, Southern Connecticut State University

Jason Henderson, Senior Associate Dean and Director of Extension, Purdue University College of Agriculture

Meredyth Hendricks, Head of Upskilling, Arizona State University

Whitney Wolfe Herd, Founder and CEO, Bumble

Jan Hochadel, President, American Federation of Teachers Connecticut

Reid Hoffman, Co-Founder, LinkedIn

Earnie Holtrey, Program Manager, Indiana Broadband Office of Lt. Governor Suzanne Crouch

Steve Huffman, Co-Founder and CEO, Reddit

Lieutenant Governor Jon Husted, Ohio (R-OH)

Larry Irving, President and CEO, Irving Group

Kelly Jin, Vice President of Community & National Initiatives, Knight Foundation

Derrick Johnson, President & CEO, NAACP

Chet Kanojia, Co-Founder and CEO, Starry

Juliette Kayyem, Belfer Senior Lecturer in International Security, Harvard Kennedy School

Daphne Keller, Director, Program on Platform Regulation, Stanford Cyber Policy Center

Senator Mark Kelly (D-AZ)

William Kennard, Chairman of the Board, AT&T, and Former Chair, Federal Communications Commission

Baroness Beeban Kidron, Founder and Chair, 5Rights Foundation

Lieutenant Governor Eleni Kounalakis, California

Callie Kozlak, Associate Superintendent for Policy & Government Relations, Arizona Department of Education

Christopher Krebs, Founding Partner, Krebs Stamos Group

Melissa Krinzman, Managing Partner & Co-Founder, Krillion Ventures

Elizabeth Laird, Director, Equity in Civic Technology, Center for Democracy & Technology

Governor Ned Lamont, Connecticut (D-CT)

Anne Marie Engtoft Larsen, Tech Ambassador, Denmark

Dr. Nicol Turner Lee, Director, Center for Technology Innovation, Brookings Institution

Jon Leibowitz, Former Federal Trade Commissioner

Blair Levin, Nonresident Senior Fellow, Metropolitan Policy Program, Brookings Institution

Lee Lewellen, President and CEO, Indiana Economic Development Association

Chris Lewis, President and CEO, Public Knowledge

Eric Loeb, Executive Vice President of Government Affairs, Salesforce

Tony London, Commissioner, Bartholomew County, Indiana

Enrique Lores, President and CEO, HP Inc.

Shannon Marimón, Executive Director, ReadyCT

Senator Edward Markey (D-MA)

Kevin Martin, Vice President of U.S. Public Policy, Meta, and Former Chair, Federal Communications Commission

Pedro Martinez, Former Superintendent of Schools, San Antonio ISD

Dr. Joe May, Chancellor, Dallas Community College District

Clare Melford, Co-Founder and Executive Director, Global Disinformation Index

Raul Moas, Senior Director/Miami, Knight Foundation

Mike Morath, Commissioner, Texas Education Agency

Satya Nadella, Executive Chairman and CEO, Microsoft

Renate Nikolay, Head of Cabinet of Věra Jourová, European Commissioner for Justice, Consumers, and Gender Equality

Alfreda Norman, Senior Vice President, Federal Reserve Bank of Dallas

Mie Oehlenschläger, Independent Tech Consultant

Irene Parisi, Chief Academic Officer, Connecticut State Department of Education

Lourdes Pereira, Student, Arizona State University

Mike Perleberg, Executive Director, One Dearborn, Inc.

William Perrin, Trustee, Carnegie UK Trust

Nate Persily, Co-Director, Stanford Cyber Policy Center

Sundar Pichai, CEO, Alphabet

Nick Pickles, Senior Director, Global Public Policy Strategy, Development and Partnerships, Twitter

Jeff Plasterer, Executive Director, Eastern Indiana Regional Planning Commission

Michael Powell, Former Chair, Federal Communications Commission

Madeline Pumariega, President, Miami Dade College

Arti Rai, Faculty Director, The Center for Innovation Policy at Duke Law

Andrea Renda, Senior Research Fellow and Head of Global Governance, Regulation, Innovation, and the Digital Economy, Center for European Policy Studies

Anthony Rendon, Speaker, California State Assembly

Chris Riley, Senior Fellow of Internet Governance, R Street

Brian Roberts, Chairman and CEO, Comcast

Mark Rosenberg, Former President, Florida International University

Jessica Rosenworcel, Chair, Federal Communications Commission

Wynn Rosser, President and CEO, TLL Temple Foundation

Deb Roy, Executive Director, MIT Media Lab

Chris Rush, Director of Educational Technology, U.S. Department of Education

Charlene Russell-Tucker, Acting Commissioner of Education, Connecticut State Department of Education

Marietje Schaake, International Policy Director, Stanford Cyber Policy Center

Christel Schaldemose, Member, European Parliament (MEP)

Carmen Scurato, Associate Legal Director and Senior Counsel, Free Press

Angela Siefer, Executive Director, National Digital Inclusion Alliance

Dr. Christina Silcox, Digital Health Policy Fellow, Duke-Margolis Center for Health Policy

Nick Simmons, Senior Advisor to the Secretary for School Reopening and Recovery, U.S. Department of Education

Sabina Sitaru, CIO, Aquiline Drones

Rebecca Slaughter, Federal Trade Commissioner

Brad Smith, Vice Chairman and President, Microsoft

Breanna Smith, Student, Arizona State University

Jim Hagemann Snabe, Chairman, Siemens and Maersk, and Chairman, Danish Digitisation Partnership

Gigi Sohn, Distinguished Fellow, Georgetown Law Institute for Technology Law & Policy

Ashkan Soltani, Executive Director, California Privacy Protection Agency

John Stankey, CEO, AT&T

Josh Stein, Attorney General, State of North Carolina (D-NC)

Dr. Hina Talib, Associate Professor of Pediatrics and Adolescent Medicine Specialist, Children's Hospital at Montefiore

Nicole Umayam, Digital Inclusion Librarian, Arizona State Library Archives and Public Records

Ed Vaizey, Member, House of Lords, United Kingdom

Cyrus Vance, Former Manhattan District Attorney

Margrethe Vestager, Executive Vice President for A Europe Fit for a Digital Age and Commissioner for Competition, European Commission

Hans Vestberg, CEO, Verizon

Dr. Eugene Washington, Chancellor for Health Affairs, Duke University and President and CEO, Duke University Health System

Tom Wheeler, Former Chair, Federal Communications Commission

Susan Wojcicki, CEO, YouTube

Jacky Wright, Chief Digital Officer, Microsoft

Carol Yeend, Co-Chair, Rush County Broadband Task Force

Andy Yen, Founder and CEO, ProtonMail

Lindsay Erin Young, Assistant Professor of Health Communication and Communication Networks, USC Annenberg Center

Eric Yuan, Founder and CEO, Zoom

Amy Zegart, Morris Arnold and Nona Jean Cox Senior Fellow, Hoover Institution, and Professor of Political Science, Stanford University

Jonathan Zittrain, Co-Founder and Director, Berkman Klein Center for Internet & Society, Harvard Kennedy School

Mark Zuckerberg, Founder, Chairman, and CEO, Meta

We also consulted staff at the following organizations:

National Conference of State Legislatures

National Governors Association

National League of Cities

Individuals' participation in town halls or interviews or the appearance of their quotations in this document do not constitute their endorsement of Future of Tech Commission recommendations.

FUTURE OF TECH NATIONAL POLLS

POLL ON TECH POLICY BY BENENSON STRATEGY GROUP: FEBRUARY 2022

Methodology:

Benenson Strategy Group conducted 1,003 interviews with registered voters nationwide from Jan. 28–Feb. 3, 2022. Interviews were conducted via traditional landline calling, SMS, and online panel, and the data was weighed to ensure a representative sample of this voter universe. The margin of error for the entire sample is ± 3.02 percent at the 95 percent confidence level.

Key Findings:

Voters across party lines **overwhelmingly support a range of government actions** aligned with the overarching goal of *protecting our privacy, protecting families, and protecting our future*.

- **Protecting our privacy:** Voters strongly believe that consumers should control their data, not companies. They widely support regulations that would strengthen privacy protections for everyday people on the internet, making it easier for consumers to control their personal data and keep it out of the hands of big tech companies that already reach too far into their lives.
 - » 78 percent support (58 percent strongly support) requiring companies to allow consumers the right to “opt-in” before sharing any of their personal data.
 - » 76 percent support (52 percent strongly support) restricting companies from collecting and using personal data beyond what’s needed for effective service.
- **Protecting families:** Voters enthusiastically back government action to ensure children and teens can use the internet safely. There is widespread support for regulations that recognize the potential for the internet to put children in danger online and prevent big tech companies and bad actors from exploiting children and their personal information.
 - » 75 percent support (59 percent strongly support) prohibiting companies from collecting personal data on anybody 16 or under.
 - » 75 percent support (49 percent strongly support) requiring tech companies to monitor the impact of their products on children’s safety and well-being to ensure they do not push inappropriate or harmful content.
- **Protecting the future:** Voters want the government to take decisive action to strengthen cybersecurity and regulate dangerous content online because, with the right protections, they believe that technology can and should be a safe force for good, moving forward.
 - » 74 percent support (48 percent strongly support) the federal government committing additional resources to strengthening cybersecurity networks, so that Americans can use the internet without fear of data breaches or cyberattacks.
 - » Voters believe misinformation online is nearly as big of a threat to the country as a data breach by foreign adversaries. 75 percent agree (40 percent strongly agree) that if the United States does not establish rules and guardrails around dangerous or false content online, our democracy could be under threat.

85 percent of American voters agree that technology is an essential element of our lives—and that the government has to regulate it just like any other essential part of life.

Overall, there is strong, widespread, bipartisan support for a comprehensive tech policy plan that would take the actions described above to protect privacy, protect families, and protect the future. 77 percent of voters support a comprehensive plan (compared to 74 percent in July 2021), including 74 percent of independents and 69% of Republicans.

POLL ON TECH POLICY BY BENENSON STRATEGY GROUP AND PUBLIC OPINION STRATEGIES: SEPTEMBER 2021

Methodology:

Benenson Strategy Group and Public Opinion Strategies conducted 2,016 interviews with registered voters nationwide from July 20–29, 2021. Interviews were conducted via traditional landline calling, SMS, and online panel, and the data was weighted to ensure a representative sample of this voter universe. The margin of error for the entire sample is plus or minus 2.07 percent at the 95 percent confidence level.

Key Findings:

There is a strong—and bipartisan—appetite for action on tech policy issues, especially when it comes to data privacy, cybersecurity, and holding social media companies accountable. Support for specific privacy policies engenders rare and strong support across party lines.

- Two-thirds of voters strongly agree (88 percent total agree): Tech companies should be required to ask consumers whether or not they can use their data, including 63 percent of Democrats who strongly agree, 64 percent of independents, and 70 percent of Republicans.
- And 9 in 10 voters across party lines support requiring privacy by default and design.

Although most voters feel hopeful and optimistic toward technology, there are grave concerns about how these issues will affect their daily lives. More than half of voters (62 percent) believe they are “likely” to be the victim of a cybercrime within the next five years.

- The idea that cybercrime is imminent and inevitable for most Americans creates a sense of urgency on the part of the government to act.

Despite these pervasive concerns, voters feel ill-equipped to protect themselves—68 percent find it difficult to protect their personal data and privacy.

- Critically, less than half of voters trust that mitigating steps—like adjusting privacy settings on devices and in apps, changing passwords

regularly, or using two-factor authentication—will actually protect their personal data and privacy.

Consequently, voters are united in their desire for the federal government to protect consumers from big tech power. Technology companies’ reach into Americans’ lives has expanded dramatically, triggering a very human reaction and backlash (“maybe they know too much”).

42 percent of voters strongly agree (80 percent total agree): The federal government needs to do everything it can to curb the influence of big tech companies that have grown too powerful and now use our data to reach too far into our lives.

- Democrats: 40 percent strongly agree / 83 percent total agree
- Independents: 38 percent strongly agree / 80 percent total agree
- Republicans: 47 percent strongly agree / 78 percent total agree

There is widespread support for strengthening anti-trust laws to ensure more competition in the technology market—83 percent of voters overall support this policy, including 85 percent of Democrats, 80 percent of independents, and 82 percent of Republicans.

- However, proceed carefully with trust-busting language: “Breaking up big tech companies” drops to the bottom of voters’ policy priority list.

When it comes to big tech, “regulation” is welcome—not a dealbreaker. 41 percent of voters strongly agree (82 percent total agree): After years of unchecked growth, we need to do more to regulate big tech.

- Democrats: 38 percent strongly agree / 83 percent total agree
- Independents: 34 percent strongly agree / 82 percent total agree
- Republicans: 49 percent strongly agree / 81 percent total agree

GENERAL SENTIMENT TOWARD TECHNOLOGY

Americans are more optimistic about the next generation of tech advancements than they are about the future of America generally.

- 57 percent of voters say the next generation of technology advancements makes them more hopeful and optimistic about the future; 42 percent say it makes them more anxious and concerned.
- 51 percent of voters are optimistic about how things will go in America over the next few years; 49 percent are pessimistic.

This optimism largely comes from the acknowledgment that people today—and especially our children tomorrow—need technology and technological skills to get ahead and succeed.

- 73 percent of voters believe that technology will make the lives of young people easier than their parents' lives (33 percent a lot easier); just 27 percent believe it will make their lives harder.
- 54 percent strongly agree (89 percent total agree): Understanding how to use technology is essential for most of our workforce.
- 44 percent strongly agree (82 percent total agree): We need universal access to high-speed internet to ensure our kids get the education they need to compete and win in a global economy.
- 36 percent strongly agree (73 percent total agree): Access to high-speed internet is as critical to families today as running water and electricity.

Still, concerns persist—especially when it comes to the impact technology will have on our national security and our personal privacy.

- Although a majority (59 percent) agree that the pace of technological change makes me feel like I'm falling behind instead of getting ahead, the sentiment is soft (only 22 percent strongly agree).
- And concerns about our susceptibility to foreign hackers or the impact of social media are far more top-of-mind and intense.

- 55 percent strongly agree (88 percent total agree): One of the biggest threats to our national security is a data breach by foreign adversaries.
- 52 percent strongly agree (84 percent total agree): I am very nervous about the effects social media is having on kids today.

For the greatest democracy and most powerful country on earth, the United States is falling short when it comes to being prepared to address technology issues.

- Nearly 4 in 10 voters (37 percent) believe the United States is less prepared than other countries to address the biggest technology issues facing society today (62 percent believe more prepared).
- And when asked whether the U.S. is more or less prepared to handle a major attack on its computer systems, 45 percent believe the
- U.S. is less prepared than other countries, with just 53 percent of Americans believing we are more prepared, and 2 percent don't know.

National cybersecurity is the top cyber-issue priority for voters, who overwhelmingly believe a foreign cyberattack is imminent—81 percent of voters believe it is likely (40 percent very likely) that in the next five years the United States will be a victim of cybercrime, where the country's critical infrastructure is hacked by a foreign adversary.

- 59 percent are very concerned (87 percent total concerned) about a cyberattack that exposes sensitive national security information to our foreign adversaries.
- 49 percent strongly agree (84 percent total agree): I am scared by the number of ways foreign adversaries can hack our data and threaten critical national infrastructure.
- 45 percent strongly agree (83 percent total agree): I am scared by the number of ways foreign adversaries can hack our data and undermine our democracy.

COMPARATIVE ISSUE PRIORITIZATION AND ROLE OF THE FEDERAL GOVERNMENT

In the full spectrum of policy priorities, security concerns around both national infrastructure and personal data are extraordinarily important to Americans across demographic groups. Other tech-related planks—strengthening privacy laws; holding social media companies accountable; expanding high-speed internet—fall behind the economy, traditional infrastructure, climate change, and health care.

- › Foreign hacking is clearly the biggest concern, but past that, there is room to focus on the positives that technology can be used for.

	% Extremely important priority (7)	% DC devotes too little attention (NET 1-3)
Preventing foreign adversaries from hacking our national infrastructure	58	56
Preventing foreign adversaries from hacking and harvesting my personal data	55	53
Supporting small businesses	47	53
Repairing our roads, bridges, and public transportation systems	47	53
Creating more good paying jobs	44	53
Combating climate change	37	42
Expanding Medicare access to all Americans	36	42
Strengthening federal data and technology privacy laws	33	48
Holding social media companies accountable for the content on their platforms	31	44
Expanding access to high-speed internet in rural America	31	43
Expanding access to high-speed internet	30	39
Providing a path to citizenship for undocumented immigrants	21	31
Breaking up big tech companies	20	43

Although technological national security concerns are at the top of Americans' priority list, voters do not believe the federal government is giving this issue enough time and attention—over half of voters say politicians in Washington are devoting too little attention.

There's an appetite for additional federal attention on technology issues, with a narrow majority placing tech and privacy issues on the federal docket. Unsurprisingly, Republicans are not as keen on giving the current administration more responsibility...

	All Voters	Democrats	Independents	Republicans
It should be the federal government's responsibility to address technology and privacy issues because these challenges will require top-level resources and expertise.	55	65	54	43
State and local governments should be responsible for addressing technology and privacy issues because they understand the needs of their constituents and can get things done more efficiently.	44	34	44	54

but nevertheless, see the need for real action to address these issues.

% Strongly Agree / % Total Agree	All Voters	Democrats	Independents	Republicans
The federal government needs to do everything it can to curb the influence of big tech companies that have grown too powerful and now use our data to reach too far into our lives.	42 / 80	40 / 83	38 / 80	47 / 78
Legislators need to create more effective laws to address technology and privacy issues.	40 / 83	43 / 85	42 / 81	35 / 82
President Biden and his administration aren't doing enough to prioritize technology and privacy issues.	26 / 63	19 / 56	23 / 62	38 / 71

We also begin with broad support for a tech policy plan—74 percent support—but support is relatively soft, with just 29 percent “strongly supporting” the plan. Democrats are fully onboard with a robust tech policy agenda, but independents and Republicans need more convincing—they support individual policies, but are less eager to create yet another comprehensive package.

- Democrats: 42 percent strongly support / 86 percent total support
- Independents: 21 percent strongly support / 69 percent total support
- Republicans: 22 percent strongly support / 66 percent total support.

Description of a potential tech policy plan: This plan would address some of the most urgent tech policy challenges and opportunities facing America’s economy, democracy, and the nation’s children and families. These include protecting the safety of Americans on online platforms, ensuring consumer privacy, fostering market competition, advancing innovation, and promoting digital equity for all Americans. This plan would also invest \$70 billion to develop future-proof broadband and provide universal access.

As we’ve seen with traditional infrastructure and other issues, “in an ideal world” voters prefer tech policy be created via congressional action.

- As the party in power, Democrats are obviously happy to let the executive branch take the lead. But voters more broadly recognize that there are more teeth in law.

	All Voters	Democrats	Independents	Republicans
The Biden administration should use executive orders to address tech policy even if it means they won’t have bipartisan support.	42	63	37	21
Addressing tech policy issues should require congressional action even if it takes longer to see results.	57	36	62	77

However, at the end of the day most voters want to see something done, even if it means the administration goes at it alone. 67 percent of voters agree with the statement, I’d rather see the Biden administration take executive action to address tech policy issues than no action at all.

- 88 percent of Democrats agree, 66 percent of independents agree, and even 44 percent of Republicans agree.

POLICY SUPPORT AND DEVELOPING OUR “BIG TENT”

Among a long list of potential policies, privacy initiatives are most popular, along with platform accountability and equity-focused policies like digital citizenship and broadband competition.

- › Republicans are especially supportive of privacy by default and design and of holding social media companies accountable.

TOP PERFORMING POLICY ISSUES

% Strongly Agree / % Total Agree	All Voters	Democrats	Independents	Republicans
Require ‘privacy by default and design’ to ensure websites/ companies ask explicit permission to use or share personal information	54 / 89	55 / 88	50 / 85	56 / 93
Update and expand special privacy protections for children	53 / 85	61 / 89	50 / 79	47 / 86
Hold social media companies accountable for illegal and harmful content posted on platforms, including misinformation, harassment, etc.	50 / 80	54 / 79	43 / 82	52 / 81
Make schools ‘privacy zones’ online	47 / 85	51 / 86	43 / 84	48 / 86
Enforce user protections on online platforms for things like hate speech, harassment, etc.	46 / 85	53 / 89	35 / 78	49 / 85
Teach digital citizenship skills in school	42 / 82	51 / 86	38 / 81	35 / 78
Enact regulations the enable a competitive, affordable broadband market	41 / 83	44 / 86	39 / 81	38 / 81

Personal Data and Privacy

Across the Future of Tech Commission’s five pillars, privacy stood out as the clear priority for voters, with the security of their personal data at the top of their list of concerns, and policies strengthening privacy protections garnering the broadest and strongest support.

- 49 percent of voters are very concerned about protecting their and their family’s personal data and privacy (83 percent total concerned).
- More than 6 in 10 voters believe they are “likely” to be the victim of a cybercrime within the next five years.

Despite intense concern about data protection, over two-thirds (68 percent) of voters find it difficult to protect their personal data and privacy.

- What’s more, less than half of voters trust that mitigating steps—like adjusting privacy settings on devices and in apps, changing passwords regularly, or using two-factor authentication—will actually protect their personal data and privacy.
- 45 percent trust (NET 5-7) that these steps will protect their data, 27 percent are neutral (4 out of 7), and 27 percent don’t trust (NET 1-3).

Whether talking about hacking and cybercrime, or companies using personal data today, voters see stronger privacy protections online as a common-sense reform.

- Two-thirds of voters strongly agree (88 percent total agree): Tech companies should be required to ask consumers whether or not they can use their data.
- Including 63 percent of Democrats who strongly agree, 64 percent of independents, and 70 percent of Republicans.

What to Do About Big Tech: Market Competition and Platform Responsibility

A slim majority of voters say the technology industry is not competitive; independents and Republicans are more likely to call out anti-competitive behavior.

	All Voters	Democrats	Independents	Republicans
Some people say the technology industry today is not competitive because a handful of very large companies dominate the sector, making it very difficult for new companies or start-ups to compete.	53	50	55	56
Other people say the technology industry today is competitive because even the big companies are constantly competing to release new products and smaller start-ups compete and succeed all the time.	46	48	44	44

Proceed carefully with trust-busting language: Breaking up big tech companies drops to the bottom of voters' policy priority list. They're not yet sold on the need for it, at least not without hearing more about the material benefits that this could have for their lives.

- This is not to say “do nothing.”
- There is strong agreement around the need to regulate big tech. 41 percent of voters strongly agree (82 percent total agree): After years of unchecked growth, we need to do more to regulate big tech companies.

There is significant enthusiasm for platform responsibility and accountability when it comes to misinformation and harassment. Highlighting the specific harms that occur on and because of social media—particularly with children—is key to generating support for action, beyond broader language about their market power.

Innovation

There is broad buy-in to the vision of technology as a force for progress. 9 in 10 agree that technological innovation will transform the way our kids live, work, learn, and connect with each other, with 55 percent strongly agreeing.

Out of more than a dozen innovations tested, voters see telemedicine services and educational technology, such as expanded remote tutoring access and modernized computer software, as the most important for government investment.

Digital Equity

Encouragingly, voters don't view technological innovation only through an entrepreneurial prism—they see investment in technology as a way to level the playing field, too.

- 85 percent of voters (including 80 percent of Republicans) agree that we should do everything we can to ensure technology is a force for opportunity and equity for all Americans.
- Don't shy away from messaging investment in technology through a fairness lens, showcasing how it can lift up Americans of all backgrounds and beliefs.

ACKNOWLEDGEMENTS

The Future of Tech Commission gratefully acknowledges the generous support of:

The Coulter Family Foundation

Craig Newmark Philanthropies

John S. and James L. Knight Foundation

The Commission's work was supported by a team of dedicated staff and advisors, including:

Colin Crowell, Senior Advisor

Sara Egozi, Staff Director

Annabelle Ison, Ison Design

Jamie Miller, Launch Director

Josh Pollack, Policy Advisor

Susan Wels, Writer

