Every four years, U.S. political parties convene to write a platform that states the beliefs and policy priorities that govern the party. New America's Open Technology Institute (OTI) submits these comments to inform this process. We recognize that this process comes at a difficult time for the world, but as the COVID-19 crisis has laid bare many inequities in our society, including access to technology, our recommendations are all the more timely.

Throughout our 11-year history, OTI has worked to ensure that every community has equitable access to digital technology and its benefits. We promote universal access to communications technologies that are both open and secure, using a multidisciplinary approach that brings together advocates, researchers, organizers, policymakers, and private-sector innovators.

Leveraging this experience, we urge the parties to develop 2020 platforms that recognize the importance of technology policy and embrace the values of equity, security, and transparency. Specifically, we make the following recommendations:

1. Protect Digital Equity During COVID-19
2. Restore Net Neutrality
3. Ensure Universal Access to the Internet
4. Make Internet Service Affordable
5. Legalize Municipal Broadband
6. Strengthen Antitrust Enforcement in Digital Markets
7. Protect Consumer Privacy and Civil Rights Online
8. Preserve Strong Encryption
9. Reform Government Surveillance Laws
10. End the Unchecked Use of Police Surveillance Technologies
11. Preserve Freedom of Expression Online While Holding Platforms Accountable

Protect Digital Equity During COVID-19. The COVID-19 pandemic has disrupted life for billions of people and prompted a variety of government actions to combat the virus and its economic fallout. Technology can play a role in fighting the pandemic, but the U.S. government must ensure that its COVID-19 response does not unnecessarily increase surveillance, exacerbate digital inequities, or leave behind the millions of people suffering through the pandemic without access to the internet.

- ➔ The use of smartphone apps in contact tracing systems must follow the demands of public health officials, not law enforcement officials or technology companies. Any contact tracing regime that incorporates digital tools should include robust protections for privacy and cybersecurity, as well as plans to ensure equitable access to the tools.
- ➔ The pandemic should not justify new, permanent surveillance regimes or exacerbate inequities in over-surveilled communities.
- ➔ The government should only collect data that it actually needs to combat the pandemic. Any new data collections must be time-limited to end after the public health emergency subsides and include strict safeguards for privacy and civil liberties.
- ➔ The federal government should establish a subsidy, discount, or voucher program to ensure that everyone can connect to the internet at home during lockdowns.
- ➔ Schools should be allowed to use federal E-Rate funding to connect K-12 students to the internet at home. The government should leverage the Pell Grant program to ensure that college students are connected when universities shut down.
- ➔ Internet service providers (ISPs) should be barred from shutting off a customer's internet service during the pandemic.

Restore Net Neutrality. In 2017, the Federal Communications Commission sparked a nationwide outcry when it repealed the federal net neutrality law, known as the Open Internet Order, and deregulated its authority over ISPs like AT&T and Comcast. With no federal cop on the beat, ISPs have been free to throttle firefighters during wildfires, stifle competition with "zero-rating" schemes, and exacerbate the digital divide without fear of government oversight. We must restore net neutrality in the United States.

- ➔ Reinstate the Open Internet Order or equivalent rules. The rules must include a ban on paid prioritization, access fee prohibitions, and a general conduct standard.
- ➔ Restore the FCC's legal authority to enforce net neutrality, protect internet users from future ISP abuses, and promote affordable internet access.
- ➔ Enact a federal law that prohibits ISPs from throttling the internet service of firefighters, public health workers, and other first responders during emergencies.

Ensure Universal Access to the Internet. The pandemic makes clear that the internet is an essential service, a utility akin to electricity and water. Yet many people lack connectivity because they struggle with digital literacy skills or live in areas that aren't served by

an internet provider. The government must address these access and adoption problems to fully close the digital divide and ensure that everyone in the U.S. has access to the internet.

- ➔ Ban "digital redlining," which happens when ISPs fail to offer service or under-invest in neighborhoods where residents are disproportionately low-income or people of color.
- ➔ Preserve the rights of local governments to use pole attachments, cable franchising, and other legal authorities to require ISPs to offer service to every resident.
- ➔ Strengthen Tribal consultation requirements to ensure that the government always protects Tribal connectivity needs—including access to spectrum over Tribal lands.
- ➔ Improve the FCC's broadband deployment maps so the government can correctly identify digital deserts across the country, including unserved urban neighborhoods.
- ➔ Direct the FCC to collect data on the cost of internet service and identify companies that engage in pricing discrimination on the basis of race, income, or geography.
- ➔ Create a grant program to fund the creation of digital literacy and inclusion programs.

Make Internet Service Affordable. Millions of people lack access to the internet because they cannot afford it. Indeed, internet service in the United States is among the least affordable in the world, contributing to growing inequality and a longstanding digital divide. The federal government must enact policies to lower the cost of internet service.

- ➔ Expand the Lifeline program by increasing the $9.25 monthly subsidy for telecommunications services and streamlining the enrollment process.
- ➔ Create competitive pressure to lower prices by blocking harmful ISP mergers and legalizing affordable municipal networks.
- ➔ Allocate more spectrum as unlicensed and implement spectrum sharing frameworks to fuel affordable, fixed wireless services, and public Wi-Fi networks.
- ➔ Make internet pricing transparent by mandating FCC collection of pricing data and disclosure of costs in a "broadband nutrition label" that helps consumers comparison-shop, avoid hidden fees, and know what they are paying for.
- ➔ Finish long-overdue FCC reforms to reduce the cost and need for set-top boxes, which often create hidden fees on consumer telecommunications bills.

Legalize Municipal Broadband. Community networks offer some of the fastest and most affordable internet service in the United States. Locally-owned networks save consumers money and spark economic growth, yet at least 20 states restrict or outright prohibit their existence. Large ISPs lobbied for these state laws because they fear competition from municipal networks. We must repeal these laws so every community can invest in its own infrastructure.

- ➔ Repeal legal barriers to municipal networks, including onerous tax schemes, mandatory ballot initiatives, and state bans.
- ➔ Municipal networks must be eligible—and given preference—for federal funds dedicated to broadband deployment.

Strengthen Antitrust Enforcement In Digital Markets. U.S. markets increasingly suffer from a lack of competition. The market for internet service is an oligopoly dominated by a handful of telecom companies, while large digital platforms have tightened their grip on technology markets. We need stronger enforcement of the nation's antitrust laws to create healthier markets, lower prices, and protect consumer rights.

- ➔ Block harmful mergers, prosecute anticompetitive conduct, review past deals such as AT&T/Time Warner and Sprint/T-Mobile, and unwind mergers when appropriate.
- ➔ Recognize that data acquisition motivates many mergers involving digital platforms—and closely scrutinize deals like Google/FitBit accordingly.
- ➔ Empower the FTC and DOJ with adequate resources, staff, and stronger internal guidelines that contemplate the privacy implications of tech mergers.
- ➔ Confirm judges who clearly demonstrate respect for and understanding of antitrust law.
- ➔ Freeze mergers during COVID-19 to ensure that dominant companies do not take advantage of the crisis to tighten their grip on tech and telecom markets.

Protect Consumer Privacy and Civil Rights Online. Surveillance capitalism has eroded public trust in companies to safeguard and use data responsibly. The public needs and deserves a strong federal law that protects their privacy and affords meaningful redress. Comprehensive privacy legislation is essential to ensure basic fairness, prevent discrimination, advance equal opportunity, and protect free expression.

- ➔ Enact comprehensive privacy legislation based on the Public Interest Privacy Legislation Principles and the Civil Rights Principles in the Era of Big Data. Legislation should ensure a private right of action and reflect Fair Information Practices, including data minimization and limitation; user rights such as data access, correction, and deletion; civil rights protections; and interoperability. The legislation should not preempt stronger state laws.
- ➔ Ensure that anti-discrimination and civil rights laws apply to online platforms.
- ➔ Establish and implement best practices for data portability, data minimization, data use limitations, algorithmic fairness, accountability, and transparency for data practices.
- ➔ Restore the FCC's broadband privacy rules, which were repealed in 2017.

Preserve Strong Encryption. In an age where data breaches, cyber crime, corporate espionage, and attacks by foreign nation states are an almost daily occurrence, encryption is one of the best tools that we have to protect ourselves and our national security. Our society and economy rely upon strong encryption for secure online communications, commerce, and so much more—particularly during the COVID-19 pandemic. Nonetheless, the DOJ, FBI, Congress, and some states have pushed technology companies to weaken their security in order to guarantee law enforcement access to encrypted communications. Such access, often referred to as a "backdoor," would leave everyone vulnerable to exploitation by cyber criminals,

foreign governments, and other bad actors. The government must stop undermining strong encryption and instead protect this critical safeguard.

- ➔ Revoke Justice Department proposals to mandate that companies build encryption backdoors into their products or services.
- ➔ Reject legislative attacks on strong encryption.
- ➔ Promote and support broad adoption of encryption by individuals, businesses, and government agencies.

Reform Government Surveillance Laws. Today, nearly every aspect of our lives is recorded or tracked by digital technologies, making it increasingly important that our personal information is protected by strong safeguards in our surveillance laws. The laws and authorities governing U.S. intelligence and law enforcement agencies enable excessive surveillance in violation of the Fourth Amendment. Government surveillance must be narrowly tailored to the goals of public safety and national security. We need strong safeguards and robust oversight for government surveillance, which often sweep up substantial quantities of Americans' communications—this will require significantly reforming our current surveillance laws.

- ➔ End the backdoor search loophole that currently allows intelligence agencies to conduct warrantless searches through data collected under Section 702 of the Foreign Intelligence Surveillance Act (FISA) when seeking information about Americans.
- ➔ Expand the role of the FISA Court amicus to advise the judges on privacy safeguards and increase accountability for government activities under FISA.
- ➔ Codify that the Supreme Court's ruling in *Carpenter v. United States*, which requires the government to obtain a warrant in order to access highly sensitive location information, applies to intelligence investigations as well.
- ➔ Require that notice be given to criminal defendants when evidence is derived from FISA authorities.
- ➔ Codify the end of the privacy-invasive and ineffective Section 215 Call Detail Records program.
- ➔ Modernize the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, and other outdated laws to fill gaps and uphold the spirit of the Supreme Court's ruling in *Carpenter v. United States*.

End the Unchecked Use of Police Surveillance Technologies. Law enforcement agencies at the federal, state, and local levels acquire and use surveillance technologies such as drones, automatic license plate readers, cell site simulators, body cameras, and facial recognition systems without any authorization. Such technologies are mostly acquired and operated in secret with minimal, if any, regulation, oversight, or community awareness. This unchecked use of police surveillance technologies is an invasion of privacy, has a chilling effect upon free speech, is often biased against women and people of color, and is disproportionately used in already-overpoliced Black and Brown communities.

- ➔ Ban law enforcement use of facial recognition and other biometric surveillance technologies, which are biased against women and people of color and inherently antithetical to the First and Fourth Amendments.
- ➔ Implement strong oversight and transparency laws that set clear standards for the acquisition and use of police surveillance technologies.
- ➔ Reexamine and minimize the use of police surveillance technologies, which disproportionately impact communities of color.

Preserve Freedom of Expression Online While Holding Platforms Accountable. Online platforms have become de facto public squares and gatekeepers of freedom of expression. The First Amendment protects online speech and imposes strict limits on the extent to which the government can direct platforms to regulate speech on their services. However, platforms must be held accountable for removing harmful content online while protecting the free expression of users. In addition, law enforcement tactics — like infiltrating and monitoring social media networks and issuing content takedown demands — threaten to chill First Amendment rights.

- ➔ Oppose new government mandates for content takedowns on social media platforms, to regulate what content may appear online, or to otherwise threaten freedom of expression online.
- ➔ Rein in law enforcement and intelligence community monitoring of social media and their ability to infiltrate platforms for investigations.
- ➔ Uphold the role of Section 230 of the Communications Decency Act in safeguarding users' speech, without permitting platforms to use the law as a shield against accountability for their own discriminatory or otherwise harmful conduct.
- ➔ Clarify that all offline anti-discrimination statutes apply in the digital environment. Where gaps exist, enact appropriate legislation.
- ➔ Hold platforms accountable to combat misinformation and disinformation on their services, especially where related to civic engagement.
- ➔ Enact rules to require greater transparency from online platforms, including regular reporting regarding their content moderation, ad targeting and delivery, algorithmic curation, and commerce policy enforcement efforts.