Report Forthcoming

Digital Safety & Investment in Internet Adoption and Use

Greta Byrum and Ever Bussey

US states are currently poised to unlock tens of billions in broadband funding from the Infrastructure Investment and Jobs Act (IIJA) – a historic investment intended to ensure that all US residents have access to the benefits of the internet. Every state is currently creating a plan explaining how it will spend funds to build broadband networks, connect residents to low-cost internet subscriptions, and ensure that residents have the devices, skills and resources needed to leverage the benefits of the digital world.

States' investments are happening at a moment when concerns about digital safety are also reaching new levels, and as:

- the Biden administration advances policies to guard Americans from the risks and dangers of AI, as well as the mental health risks of social media and other forms of digital engagement;
- the Federal Trade Commission and Federal Communications Commission consider rulemakings on digital privacy and safety; and
- philanthropies—including the Ford Foundation, MacArthur Foundation, Omidyar, Mindaroo, and others—support the work of lived experts addressing digital safety for those experiencing tech-enabled discrimination, surveillance, disinformation, hate, fraud, and harassment.

As states develop their digital equity plans, they are also finding that the vast majority of their residents are concerned about digital privacy, security, and safety. In New York State, for example, 87% of residents surveyed in 2023 are either somewhat concerned or very concerned about their online safety, including 92% of aging individuals. Focus groups across states find a range of concerns including online scams and fraud, hate and harassment, misuse and theft of data, and surveillance and discrimination. People find that all of it is overwhelming and leads towards a general "technophobia" when it comes to using the internet at all.

A forthcoming study from Benton Institute for Broadband & Society Fellow Greta Byrum and co-author Ever Bussey shows that, based on evidence from state digital equity plans, safety concerns keep people from adopting and using the internet. Further, the study shows that internet adoption without support and knowledge of digital risks leads to actual harm not only to individuals but to social, civic, and financial systems.

Greta Byrum

A Principal for Broadband and Digital Equity at HR&A Advisors, Byrum is a veteran of the Digital Equity space. She is working with people & tech to envision and build just and resilient communications systems. As a Marjorie & Charles Benton Opportunity Fund Fellow, Byrum is developing strategic guidance for how state digital equity plans can help new and historically marginalized users navigate the internet safely.

Ever Bussey

Bussey is a social researcher and creative media maker. Ever was introduced to digital media making through Allied Media Projects, where they learned to apply a social justice lens to their creative practice. They were able to expand their background in creative media and Participatory Action Research while pursuing graduate studies at The New School, where they received their MA in media studies.

BENTON INSTITUTE for BROADBAND & SOCIETY

Marjorie & Charles Benton Opportunity Fund

Experts Interviews

Tawana Petty, Just Tech Fellow and Founding Director, Petty Propolis

Aki Younge, Director of Movement Collaborations, UCLA Center on Race and Digital Justice

Sandra Ordonez, Bronx native Latina, internet freedom activist for over 2 decades, and Head of Team, Team CommUNITY

Daniel Khan Gillmor, Senior Staff Technologist, Speech Privacy and Technology Project, American Civil Liberties Union

Sarah Aoun, Security and Privacy Researcher

Una Lee, Creative Director, And Also Too

Leigh Honeywell, CEO and Co-Founder, Tall Poppy

Myeong Hong-Hurwitz, Founder, Tiny Gigantic

Seeta Peña Gangadharan, Associate Professor, London School of Economics

To conduct the study, Bussey and Byrum reviewed IIJA-funded state digital equity plans and interviewed leading digital safety and security experts, many from communities most at risk from digital harms. These experts also suggest concrete steps that government officials, philanthropy, and communities can take to reduce risks for new and vulnerable internet users using the "power, not paranoia" approach articulated by the data privacy group Our Data Bodies.

> *"Rather than putting the burden of digital self-protection on individuals, to collectively examine connections and patterns so we can begin to imagine and develop creative tools and practices that will advance our communities from paranoia to power."*

The researchers, community organizers, technologists, and strategists quoted in the report have invested decades in preparing and protecting individuals and communities from online threats and harms including hate, harassment, discrimination, and surveillance, in addition to the more widely understood risks of data theft, misuse and cybercrime. They stress that risks and harms are systemic. Training individuals in password protection basics is not enough. Seeta Peña Gangadharan, co-founder of Our Data Bodies, said,

> *"You can't just teach someone how to use a password manager and think they're going to be fine. We can teach data privacy literacy till we're blue in the face, but if at the organizational level we're failing to make smart vendor and procurement choices, and if we haven't spoken with our patrons, clients, communities, or publics about their privacy, safety, and security needs in an ongoing basis, then we're missing the point."*

Those who work every day with victims of digital harm cite increased threats and risk for new internet adopters. Just Tech Fellow and decades-long Detroit organizer Tawana Petty explains that aging individuals, Black and Brown communities, those with low levels of literacy or limited English, people living with disabilities, veterans and other less connected groups (who include many of the covered populations under IIJA) are "especially vulnerable to fraud through the use of deep fakes and vocal replication tech, and are often spammed in ways that allow access to their bank accounts."

Experts also cite disproportionate use of surveillance and social control over communities who are already hyper-surveilled by law enforcement and credit systems. "We're moving toward a social-credit system where the "undesirable" population are being contained in surveillance mechanisms," says Petty. Digital safety services company CEO Leigh Honeywell stresses that threats come from many different kinds of actors, citing extremists, malicious actors online who are not specifically acting out of political motivation but sociopathy; online stalking or harassment by former intimate partners, ex-employees, or fans; and foreign and domestic actors perpetrating scams and fraud.

Experts caution that online safety isn't a matter of protecting individuals only. "This runs the gamut of one person in an organization dealing with it on a personal level or a whole organization dealing with it by being spear phished," says Myeong Hong-Hurwitz, founder of digital safety service provider Tiny Gigantic. Sandra Ordonez, Team Lead for Team CommUNITY says: "Efficiencies of scale favor bad actors" – and the internet is a key driver for efficiencies of scale.

Overall, says Ordonez, we are facing a "diverse threat landscape, but many developers, officials, and policymakers don't fully understand the context of vulnerable users, and don't have the cultural sensitivity" to fully explore and develop the urgent solutions that are needed.

Byrum and Bussey's report will suggest a set of fundable solutions that philanthropy and government officials should apply in order to best leverage IIJA funds to fully respond to the diverse threat landscape faced by new and vulnerable internet users.

Design Legislative, Procurement, and Grantmaking Solutions

- Create standards and policies applied to procurement and grantmaking processes include data retention and data breach policies, the requirement of duty of care for people in high-risk jobs, and device and network standards, for any activity receiving IIJA funds;
- Build diverse tech talent and projects that are community based, by providing scholarships and workforce pipelines that prioritize participation from most impacted communities who are familiar with the context and experience of digital harms.

Invest in Training and Community Support Solutions

- Libraries, public computer centers, and community hubs which serve as front-line digital inclusion resources to provide culturally sensitive digital hygiene training and support, addressing underlying knowledge gaps that make it difficult for new and late adopters to recognize threats and harms;
- Groups and organizations that are typically targeted due to political activity or belonging to a group targeted by hate and harassment, to conduct risk assessments and prepare forward-looking plans and conduct ongoing conversations;
- Institutions and ecosystems, including wraparound service providers such as housing, school, and workforce institutions, as well as organizations and entities already doing this work in communities;
- Trusted intermediaries supporting communities and individuals facing digital risks to conduct audits including bug reporting, monitoring, software maintenance, and daily tech support. These interlocutors should work directly with communities but be empowered to identify and report larger problems to state agencies or other funders.

The forthcoming report will include resources for funders and government officials interested in supporting holistic approaches to digital safety, especially for new and vulnerable internet users, including model policy language and a resource library of solutions and precedent examples.

With proper attention to issues of safety and trust, the IIJA can provide an unprecedented opportunity to not only close the digital divide, but to ensure that people just coming online are protected, safe, and confident as they build their digital lives.