# BUILDING SAFETY INTO DIGITAL INCLUSION EFFORTS

## RISKS AND OPPORTUNITIES IN THE DIGITAL EQUITY ACT

By GRETA BYRUM

Published by the BENTON INSTITUTE for BROADBAND & SOCIETY

SEPTEMBER 2024

# BUILDING SAFETY into DIGITAL INCLUSION EFFORTS: RISKS and OPPORTUNITIES in the DIGITAL EQUITY ACT

By Greta Byrum

Collaborating Author: Ever Bussey

Contributing Editor: Revati Prasad, PhD

BENTON
INSTITUTE
for BROADBAND
& SOCIETY

Broadband Delivers Opportunities
and Strengthens Communities

1041 Ridge Road, Unit 214
Wilmette, IL 60091
benton.org

Please include the following attribution when citing this report: Byrum, Greta, “Building Safety Into Digital Inclusion Efforts: Risks and Opportunities in the Digital Equity Act“ Wilmette, IL: Benton Institute for Broadband & Society, September 2024. benton.org/publications/digital-inclusion-safety

# CONTENTS

# EXECUTIVE SUMMARY

As more and more essential services and activities move online, people have less and less of a choice about whether or not to participate in the digital world. Yet expanded internet use can bring with it increased risk.

Currently, unprecedented levels of investment in digital equity and broadband deployment via the Infrastructure Investment and Jobs Act (IIJA) hold the promise of "internet for all," but a core tenet must be ensuring that new and vulnerable users are safe. While internet connectivity expands opportunity and opens doors to civic and social forums, it also compels users to agree to processes and terms they often don't understand, while at the same time dodging scams and shielding personal information from theft and misuse.

In this report, we offer recommendations to state and territory broadband offices regarding what they can do to mitigate the potential harms of an increasingly digital life, especially as they roll out programs funded by the IIJA's Digital Equity Capacity Grant Program.

These include:

- What actions broadband offices can undertake to build safety into program administration, for example:
    - Risk assessments;
    - Device and software standards;
    - Data policies;
    - Procurement of safety and virus protection applications and tools; and
    - Governance standards for use of artificial intelligence tools for administrative and programmatic purposes.

The **DIGITAL EQUITY CAPACITY GRANT PROGRAM** is a $1.44 billion formula grant program for states, territories, and tribal governments via the Digital Equity Act funding allocation under the Infrastructure Investment and Jobs Act.

- What design principles for safety and cybersecurity programs and projects broadband offices can implement, for example:
  - Prioritization of tech workforce programs that build job pipelines for marginalized and vulnerable communities, who best understand the experience of those communities;
  - Investments in holistic training and community support solutions to shift the burden of protection away from individuals and toward collective solutions;
  - Establishment of programs that go beyond password basics to address social media safety, targeted fraud and harassment, and the embarrassment and shame that can come with exploitation; and
  - Incorporation of digital safety measures into subgrant programs to ensure safety across a range of digital skills and internet uses.

We base these insights on a series of interviews conducted with leading practitioners working on digital safety with historically marginalized populations, many of whom are defined as beneficiaries or "Covered Populations" in the Infrastructure Investment and Jobs Act. Several common themes emerged from these conversations, including:

- Digital safety is a social, interpersonal, and community issue, and the most effective measures to build awareness and protect people from harm emerge in social and community settings;
- There is an urgent need for institutions—not just internet users, individuals, or policy beneficiaries—to review and update their protocols and practices in view of increased risk, given the volume of sensitive information on individuals they hold;
- Many tech developers, officials, and policymakers are not aware of the societal context of vulnerable internet users. This points towards a need for collaboration with community representatives to fully explore and develop urgently needed solutions;
- The people disproportionately exposed to fraud as well as wide-net surveillance and algorithmic bias due to membership in particular population groups—including most Covered Populations—are far more likely to be overwhelmed by and distrustful of technology than others; and

**COVERED POPULATIONS**
defined by the IIJA

-Individuals who live in covered households (with income not more than 150% of the Federal Poverty Level),

-Aging individuals (60 and above),

-Incarcerated individuals, other than individuals who are incarcerated in a Federal correctional facility,

-Veterans,

-Individuals with disabilities,

-Individuals with a language barrier, including individuals who are English learners, or have low levels of literacy,

-Individuals who are members of a racial or ethnic minority group, and

-Individuals who primarily reside in a rural area.

- The societal impact of digital privacy issues is much broader than the risk to individuals, encompassing systemic risk at many levels including damage to social and civic institutions as well as clear danger to our national financial and democratic health.

As states and territories develop implementation strategies for their digital equity plans and Capacity Grant–funded programs, the recommendations offered here can help them deliver on one of the five required measurable objectives: “Awareness of, and the use of, measures to secure the online privacy of, and cybersecurity with respect to, an individual.”

However, the Digital Equity Act and implementation of its programs alone won’t be enough. Any effort undertaken in this context must be supplemented by a broad and pervasive structural reform effort on the parts of lawmakers, civil society, and relevant agencies. Otherwise, the harms that accompany internet use could undercut every benefit that equitable broadband is supposed to provide.

# INTRODUCTION

The pandemic revealed just how critical internet use has become for basic everyday life, determining access to work, learning, social and civic participation, financial systems, and a range of other daily services. The crisis also exposed a stubborn and persistent inequity: Too many Americans still do not have reliable, quality internet access. Moreover, even those who do have internet access may face other barriers when it comes to full digital participation, including lack of quality devices, digital skills, and difficulty navigating hard-to-use online services.

In response to renewed attention placed on digital participation and the stubbornness of the digital divide, in 2021 federal and state governments mobilized to ensure that all U.S. residents are brought online and can access online services as a critical part of recovery. The Infrastructure Investment and Jobs Act, along with a handful of stimulus packages, targeted the goal of closing the digital divide with a series of historic investments. Over $60 billion in broadband assistance is currently rolling out across the country, intended to close persistent gaps in internet access and adoption. Congress set aside $1.5 billion of that funding for digital support beyond just internet access in the Digital Equity Act (DEA), which is contained in the Infrastructure Investment and Jobs Act.

Currently, all U.S. states and territories are preparing to implement their digital equity or opportunity plans. As an economic recovery, development, and equity measure, expanded internet access and use can provide greater opportunity for everyone to access online learning, health services, and employment, as well as civic and social connectedness.

In particular, plans and funded programs must include strategies, benchmarks, and targets addressing barriers to internet adoption with regard to five primary objectives:

- Access to affordable broadband service;
- Access to devices that meet the needs of users, and support for those devices;

- Access to digital literacy and skills training;
- Accessibility of online government and essential services; and
- *Awareness and the use of measures to secure the online privacy of, and cybersecurity with respect to, an individual.* [emphasis added]

Each state or territory has chosen its own methods and approaches to design programs relevant to these objectives for all residents, including the eight "Covered Population" groups who are intended primary beneficiary groups for Digital Equity Act–funded efforts. The multiplicity of approaches is bounded by the rules laid out in the DEA statute itself. The DEA also offers the potential to create a set of shared data, learnings, and strategies nationwide as broadband offices collect and publish data on internet adoption, and create and implement plans to improve digital outcomes for their residents.

At the same time, a sharp uptick in concerns about the risks of internet use is driving government and private actors to advance policies guarding Americans from the dangers associated with internet use—including fraud, data breaches, surveillance and harassment, and mental health risks.

Digital safety is a complex topic, which encompasses everyone who interacts directly with internet-enabled devices as well as those who can be exploited, marginalized, or surveilled by algorithmic and data-dependent systems.

This report is intended to address tensions between the goals of 1) expanding universal broadband access, adoption, and use to provide equal digital opportunity for all, while protecting the free and open internet; and 2) addressing the spread of fraud, cybercrime, and digital abuse, along with unchecked and unregulated expansion of inequitable application of surveillance, predictive algorithmic systems, and other risks and harms that accompany emerging technologies.

Fully addressing the spectrum of risks that accompany internet use will require a far broader effort than what is possible under the Digital Equity Act and the programs it supports. However, it is imperative that the current investments support safety for beneficiaries—and do not undercut or contradict efforts to reduce exposure to digital harms.

# METHODOLOGY

To provide a fuller picture of the state of internet safety—especially for those who have been digitally excluded, who have less exposure and thus less knowledge about digital risks and harms—we have conducted a qualitative study examining existing research conducted by states on digital safety, through:

- Desk research on the risks and harms of internet use;
- An audit of state and territory digital equity plans exploring privacy and safety assessments and proposed solutions;
- Interviews with leading digital safety practitioners and advocates working with Covered Populations and the most-impacted communities;
- Desk research compiling existing curricula and safety resources currently in use in most-affected communities;
- An October 2023 open-door interactive roundtable with Our Data Bodies, a team of leading practitioner-researchers; and
- A January 2024 private roundtable with philanthropic leaders to discuss strategies for building digital safety ecosystems.

The researchers, practitioners, community organizers, technologists, and strategists we spoke with to develop this report have invested decades of effort to prepare and protect 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, information misuse, and cybercrime. We prioritized participation by experts who are members of communities most impacted by both digital exclusion and risk, and who thus have both deep lived and professional expertise with the context as well as the needs and experiences of traditionally marginalized communities.

We interviewed **Tawana Petty**, a veteran of organizing, pedagogy, and research in this area and a leading voice in establishing human rights frameworks for emerging technologies.

## INTERVIEWEES

**Sarah Aoun** is a technologist who has worked for over 15 years with groups around the world on cybersecurity, privacy, and internet freedom, including support for journalists, human rights defenders, and high-risk individuals. Most recently, she was the vice president of security and chief technology officer at the Open Technology Fund, an organization that funds projects, research, and technology focused on countering censorship and surveillance.

**Daniel Kahn Gillmor** is senior staff technologist for the Speech, Privacy, and Technology Project of the American Civil Liberties Union (ACLU). Gillmor focuses on the way our technical infrastructure shapes society and impacts civil liberties.

**Leigh Honeywell**, CEO and cofounder of Tall Poppy, helps companies protect their employees from online harassment. She was previously a Technology Fellow at the Speech, Privacy, and Technology Project of the ACLU, and also worked at Slack, Salesforce, Microsoft, and Symantec. She has cofounded two hackerspaces, and she advises several nonprofits and startups.

**Myeong Hong Hurwitz**, Tiny Gigantic founder, is an enthusiastic breaker and maker of technology for social justice. They see holistic security as one of many superpowers social justice movements have to care for each other, be more sustainable, and stand stronger against injustice. They are a cofounder of the technology cooperative Research Action Design (rad.cat).

**Una Lee** is a design justice practitioner and organizer. In her work as founder of the Consentful Tech Project, Una advocates for technology and data collection to be based in care and consent rather than control and extraction. She is the instigator of the Design Justice Principles and a cofounder of the Design Justice Network. Una is the creative director of And Also Too, a design justice studio that prioritizes accountability to the communities it works with and within.

**Sandra Ordóñez**, Bronx native, Latina, and head of team at Team CommUNITY—has over 20 years of experience working at the intersection of technology, community engagement, and human rights. She was one of the first Latinas to occupy leadership positions in the open source community, notably having served as the first director of communications for the Wikimedia Foundation.

**Tawana Petty** is a mother, social justice organizer, poet, author, and facilitator. Her work focuses on racial justice, equity, privacy, and consent. She is a 2023–2025 Just Tech Fellow with the Social Science Research Council and a 2024 National Leading from the Inside Out (LIO) Yearlong Fellow with the Rockwood Leadership Institute. She is an alumni fellow of the Digital Civil Society Lab at Stanford Center on Philanthropy and Civil Society, the Detroit Equity Action Lab, and Art Matters Foundation. Petty currently serves as the founding executive director of Petty Propolis, a Black women–led artist incubator primarily focused on cultivating visionary resistance through policy literacy and advocacy, data and digital privacy education, and racial justice and equity initiatives.

**Akina (Aki) Younge** is director of movement collaborations at the UCLA Center on Race & Digital Justice, and she previously was director of policy innovation at Data for Black Lives. Her work spans many policy areas, including school integration, housing, workers' rights, and the future of work.

# THE RISKS AND HARMS OF INTERNET USE

The Digital Equity Act (DEA) established a call for states and territories to assess and address privacy and cybersecurity issues, especially for new and traditionally marginalized internet users. To understand the context in which the DEA will be implemented, it is important to expand and delineate the tangible potential harms that come with increased internet access.

## Fraud

Earlier this year, the Federal Trade Commission (FTC) announced that in 2023, financial losses due to internet-enabled crime and fraud topped $10 billion for the first time—a 14 percent increase over 2022. Social media–driven investment and impostor scams topped the list of risks. "Digital tools are making it easier than ever to target hard-working Americans," said Samuel Levine, director of the FTC's Bureau of Consumer Protection.[1] The FTC is combating the rise of digital harm with a series of rulemakings as well as a fraud reporting and tracking system.

Meanwhile, scams and fraud have become increasingly more sophisticated in ways that are not solvable through basic digital hygiene training for individuals. For example, in early 2024, a financial-advice columnist for New York Magazine admitted that she had been scammed out of $50,000 by fraudsters who claimed to be CIA agents protecting her from identity theft—who had, in fact, found her personal data on the internet and exploited it to trick her into eventually stuffing a shoebox full of cash and handing it to a courier.[2] And fraud and scams are not limited to explicitly criminal operations—the Federal Communications Commission (FCC) has handed out fines to several telecommunications companies for fraudulent and dishonest practices related to the Affordable Connectivity Program within the past year.[3]

**DIGITAL HYGIENE**, or self-care in the digital realm, involves a series of practices and habits aimed at safeguarding and enhancing one's digital well-being. Much like self-care routines contribute to physical and mental health, digital hygiene focuses on maintaining the health, security, and overall well-being of our digital lives.
-Dartmouth

Online fraud does not hit all populations equally:[4] 34 percent of all Americans, and 44 percent of Black adults, have experienced at least one sort of digital fraud in the past year.[5] Across political differences, most Americans (72 percent) wish for more regulation of what companies can do with people's data; just 7 percent say there should be less regulation.[6]

## Children Are a Particularly Vulnerable Group

At a January 2024 hearing on digital safety, Senate Judiciary Committee Chairman Dick Durbin (D-IL) called online child exploitation a "crisis in America" fueled by rapid changes in technology that give predators "powerful new tools" to target kids. Families spoke about social media use leading to self-harm and even suicide, in addition to expressing concerns over child sexual abuse cropping up on the internet.

The Pew Research Center reports that most Americans are concerned about social media sites knowing personal information about children (89 percent), advertisers using data about what children do online to target ads to them (85 percent), and online games tracking what children are doing while playing them (84 percent). In 2023, President Biden tasked staff from the Department of Health and Human Services and the Commerce Department's National Telecommunications and Information Administration (NTIA), to cochair the Task Force on Kids Online Health and Safety to make recommendations of actions to protect the health, safety, and privacy of minors online.

## Unease But Resignation

A 2023 Pew Research Center report demonstrates that U.S. residents are well aware of digital risks, but the majority (61 percent) are skeptical that anything they do will make a difference. Overwhelming majorities are also concerned about how companies (81 percent) and government (71 percent) use their data. Roughly three-quarters or more feel that they have very little or no control over the data collected about them by companies (73 percent) or the government (79 percent).[7] The Pew report also notes that those with the greatest knowledge about digital safety and privacy are more likely than others to take protection measures such as adjusting social media privacy settings, avoiding cookies, using a private browser or search engine, and using a password manager. Yet the majority of Americans (69 percent) feel overwhelmed by managing passwords and other basic digital hygiene measures.

According to the report, many of the most at-risk population groups are less likely to take these measures, and to articulate greater skepticism regarding the effectiveness of existing privacy-protecting measures and tools. This echoes what we heard from our interviewees: that new and historically marginalized groups often feel that they are coerced into complying with the all-powerful, pervasive forces beyond their control—but that they have no choice if they wish to access essential services and opportunities.

Some government agencies are stepping up to address conditions of risk and harm in the digital world. In addition to the Federal Trade Commission, the Federal Communications Commission is also acting on digital safety with its Privacy and Data Protection Task Force. Like the FTC, the FCC task force is taking a rulemaking and enforcement approach to govern data protection, the misuse of surveillance technology (for example, in domestic abuse situations), reporting requirements related to data breaches, and regulation of the information and communications technology and services supply chain. The FCC also adopted rules on safeguarding and securing the open internet as part of its reclassification of the internet as a Title II telecommunications service – also known as the "net neutrality" rules. These rules classify broadband internet as a means of communication or "telecommunications" rather than an "information service," thus allowing the FCC to regulate it.

## Artificial Intelligence

Even as government and civil society measures move forward, internet and data-driven technologies present new, expanding, and pervasive societal dangers. Amid all of the risks, artificial intelligence (AI) has also lately taken center stage as a concern with regard to the impact of technology on everyday life, with 81 percent of Americans expressing a belief that the use of AI will lead to unintended consequences and public discomfort, according to Pew.

Artificial intelligence deepens and expands virtually every risk, making it exponentially easier for bad actors to exploit data to defraud and harass internet users—and, additionally, to generate dis- and misinformation (including deep fakes) that threaten to derail democratic and social processes.

The use of AI and algorithmic modeling has also shown itself to carry disproportionate risk for historically marginalized populations who have already been the subjects of over-policing, including by predictive modeling

**MISINFORMATION** is the sharing of inaccurate information.

**DISINFORMATION** is the sharing of false information with a malicious intent.

**DEEPFAKES** are videos, pictures, or audio made with artificial intelligence to appear real, conveying false information about people or events.

for housing finance decisions and law enforcement.[8] The White House has sought to address these issues with the creation of a Blueprint for an AI Bill of Rights for protecting civil rights in the algorithmic age, led by former Office of Science and Technology Policy director Alondra Nelson, who said: “Algorithms used across many sectors are plagued by bias and discrimination, and too often developed without regard to their real-world consequences and without the input of the people who will have to live with their results.”

With an October 2023 Executive Order from the White House, President Biden elevated the non-enforceable Bill of Rights to a set of mandates to be adopted by all federal agencies, with oversight by the federal Office of Management and Budget. Meanwhile, states, cities, and municipal agencies are just beginning to grapple with the contours of regulation for AI systems, including their own procurement and standard operating procedures.

Those just coming online with the support of the Digital Equity Act will be faced with an irregular, unpredictable, and rapidly evolving set of interactions with data-driven tools. The impact of increasing adoption of AI on the commercial internet and by government actors is already clear in two areas of everyday life:

1. Predictive AI systems, including policing algorithms as well as criminal-justice and benefits-decision tools, have been shown to deepen bias and deny rights.[9]

   The use of predictive AI is on the rise for business and transactional purposes, including collecting and analyzing personal data to determine eligibility for social programs and public assistance—and for determining health or car insurance coverage decisions, often without the consent of the person most affected.[10] These tools are often created with proprietary metrics and parameters, making it impossible for auditors to understand how the machine learning system makes its decisions. Increased use of algorithmic decision-making tools may even make biases worse by denying standing for legal challenges where the use of proprietary AI tools creates disproportionate impact but where intention to discriminate cannot be demonstrated.

2. Meanwhile, generative or Large Language Model (LLM) AI systems—such as ChatGPT, Claude, Gemini, and Violet—carry a different set of risks. AI companies themselves predict that their tools will rapidly degrade the information environment online, making it virtually impossible to discern accurate, quality information from fabricated or inaccurate content. A degraded internet will be difficult to navigate and could further weaken trust in institutions while increasing instances of fraud and predation by making them harder to detect.

Navigation of the internet will require a new understanding of the skills and literacies needed. In the long run, we may need to replace much standard curriculum and best practices applied to digital literacy training in view of alterations coming along with AI environments. It is likely that we will have to call upon digital equity experts and technologists to assist people in determining what is legitimate content versus phishing or data harvesting.

Finally, alterations emerging from AI will also fundamentally change the nature of valued labor, also altering what skills are needed in the workforce and thus requiring a reinvention of workforce training for internet-enabled jobs.

## Disproportionate Impact

Scholars Seeta Peña Gangadharan and David Barnard-Wills have argued that many well-intentioned digital inclusion efforts often draw participants into a web of risk and danger, without providing protective guardrails.[11] [12]

New internet users face increasing risks of nonconsensual data extraction and predation on multiple levels: biases reinforced through the application of artificial intelligence; commercial surveillance—including by the same organizations and companies providing digital services; exposure to third-party tracking and data extraction; and the everyday risks of participating in digital life, including fraud and harassment. Many scholars—Ruha Benjamin, Safiya Noble, Virginia Eubanks, and Wilneida Negrón—have analyzed the ways in which data-driven systems can alienate and criminalize Black, Brown, low-income, and other historically marginalized groups. Safiya Noble has demonstrated how biased online search results can impact how people experience the internet.[13] In her book The New Jim Code, Ruha Benjamin has analyzed how new technologies can reinforce and deepen historical patterns of oppression.[14] And Virginia Eubanks and Wilneida Negrón have both shown how digital workplace surveillance and tracking tools are increasingly surveilling and tracking low-wage workers.[15] [16]

Digital Equity Act programs that bring new users online could run the risk of unintentionally deepening these injustices unless their implementers and decision makers take action to deeply and intentionally integrate safety approaches and tools.

# QUALITATIVE FINDINGS

To confirm and deepen our understandings of the vectors of risk for internet users, as well as possible solutions, we conducted a series of roundtable discussions and interviews with experts working to study and address these issues.

## Roundtable Discussions

Our first open-door roundtable, conducted in October 2023, explored a historical and policy framework for both digital equity investments and community digital safety efforts, drawing from the legacy of the 2009 Broadband Technology Opportunities Program (BTOP), the precedent federal broadband and digital equity stimulus program to the IIJA. Participants discussed learnings from the BTOP—in particular, the lack of consideration for privacy and safety in that program. Dr. Seeta Peña Gangadharan helped lead the discussion, which focused on the importance of ensuring that institutions and governments recognize and embrace their own crucial role in fostering digital safety, rather than placing the burden of cybersecurity on vulnerable individuals.

Dr. Gangadharan described how Our Data Bodies, a community research collective, offers digital tools and community events in which participants come together to develop collective agreements around how they use social media together. For example, participants discuss asking for consent before tagging others in photos, demystifying technical topics like what activities create data trails, identify activities that are perhaps safer to undertake offline, and develop norms around collective interaction with data-driven technology. As Our Data Bodies puts it, "Rather than putting the burden of

**Dr. Seeta Peña Gangadharan** is associate professor in the Department of Media and Communications at the London School of Economics and Political Science, where she also serves as deputy head of department (research) and program director for the MSc Media and Communications (Governance).

Her work focuses on inclusion, exclusion, and marginalization, as well as questions around democracy, social justice, and technological governance.

She currently co-leads two projects: Our Data Bodies, which examines the impact of data collection and data-driven technologies on members of marginalized communities in the United States; and Justice, Equity, and Technology, which explores the impacts of data-driven technologies and infrastructures on European civil society.

## A SELECTION of DIGITAL SAFETY RESOURCES

(Additional resources and more detail provided in Appendix 1.)

PRIVACY RECIPE: Creating an Online Persona: Guide to creating a private online identity.

Digital Security Flyer: Digital security tips aimed at protesters, organizers, and activists.

Digital Defense Playbook: Workbook of popular education activities focused on data, surveillance, and community safety.

Surveillance Self-Defense: Guide to protecting oneself from electronic surveillance.

A First Look at Digital Security: Open-source booklet on digital security.

Signal for Beginners: Guidebook on the secure messaging app.

Surveillance Self Defense: Tips, Tools and How-Tos For Safer Online Communications by Electronic Frontier Foundation

Precisely Private Good Privacy Practices: Best practices to better protect privacy and security online.

Defend Our Movements: Online, collaborative source of questions/answers, resources, links, and other information about protecting data.

digital self-protection on individuals, [we should] 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."[17]

Takeaways from this conversation included an affirmation that the burden of managing internet risks is too great for any individual. Collective strategy is more motivating and effective than driving people toward technical solutions on the basis of fear and concern alone.

Our closed-door roundtable for funders, conducted in January 2024, presented findings from the first roundtable as well as from the interviews, and provided recommendations for how philanthropy might make investments to steer states and territories toward safety and privacy protection in implementation of their digital equity plans. Monique Tate and Brandon Forester led this discussion.

This roundtable included examples of the avenues available to philanthropies to leverage the current federal funding opportunities to move their funding priorities—for example, health, anti-poverty, and civic and electoral participation—forward by advancing digital equity. There was also a recognition that the lack of safety in digital environments can drive down internet adoption and thus diminish the effectiveness of such investments.

**Monique Tate**, a director for Community Tech New York, educates community wireless network advocates and enthusiasts across the country.

She has introduced thousands of people to community technology and has recruited and educated hundreds in digital stewardship, community leadership, community networks, and digital justice coalition building.

From 2016 to 2020, she deployed and managed the largest community network in Detroit, for the Equitable Internet Initiative, with nine relay sites and three solar-powered Wi-Fi and charging stations; and she activated the first Detroit public park (Bennett Playground) with Wi-Fi, serving thousands.

For over a decade, **Brandon Forester**—national organizer for internet rights at Media Justice—has been an educator and organizer working on communication rights, access, and power for communities harmed by persistent dehumanization, discrimination, and disadvantage. He envisions a future in which everyone has sustained and universal access to open and democratic media and technology platforms.

# Interviews

Between July and October 2023, the authors of this report conducted a series of interviews with leading researchers, practitioners, community organizers, technologists, and strategists who have collectively invested decades of effort to prepare and protect individuals and communities in matters of digital safety.

Our interviewees have contributed to a collective understanding of how new, historically marginalized, and vulnerable internet users experience digital risks and harms. They have also contributed substantively to direct support efforts for vulnerable communities, in many cases without reliable or sufficient institutional support.

The interview script (Appendix 2) asked participants to share their views on individual and community needs for digital privacy, security, and safety support and training in the context of the Digital Equity Act. Questions focused on what interviewees have learned in their work with individuals and communities, recommendations regarding priority risks, descriptions of what officials and policymakers should know about the experiences of most-impacted communities, suggestions for what meaningful protective strategies might look like, and an estimation of what support is needed to scale successful efforts.

## INTERVIEW THEMES:

In our discussions, interviewees stressed that risks and harms are systemic, and that interventions targeted only at individual behaviors and preparedness will not adequately address systemic risks. For example, threats in this area include foreign and domestic actors perpetrating ransomware attacks on municipalities and other government agencies.

Interviewees also spoke about how those disproportionately exposed to wide-net surveillance and algorithmic bias, including racial and ethnic minorities, are far more likely to be overwhelmed by and distrustful of technology overall. Interviewees cited a lack of awareness of the context of vulnerable internet users among technology developers, officials, and lawmakers, and the need for cultural sensitivity and collaboration with community representatives to fully explore and develop the solutions that are urgently needed.

Threats come from many different kinds of actors and are not limited to risk of fraud and cybercrime. Some examples include harassment by extremists, malicious actors who are not specifically acting out of political motivation but rather sociopathy, and online stalking or harassment by former intimate partners, ex-employees, or fans.

“Unconsentful” data collection, as defined by Una Lee’s Consentful Tech Project, also presents an expanding threat, both through passive extraction (for example, cookies collected during online browsing that are then sold for ad targeting, or wide-net surveillance by law enforcement) and as a product of interaction with smart technologies and location services. Large language models ingest all manner of data, including personally identifiable information. And data breaches are frequent—and often are unreported to those affected.

The range of risks and threats that emerge with expansion of internet access and adoption is dauntingly broad and complex; the policy response to these issues is just catching up with some of them. Overall, our interviews confirmed the quantitative information revealed by the Pew surveys and published in states’ digital equity plans: interviewees and survey respondents articulate a sense of powerlessness and futility around the personal actions they may take on an individual basis relative to the full threat landscape.

Observations fell into three themes:

## 1. SHIFT THE BURDEN of DIGITAL SAFETY AWAY FROM THE INDIVIDUAL and TOWARD SOCIAL SYSTEMS and INSTITUTIONS

Our interviewees contended that whereas the Digital Equity Act frames digital safety as an issue to be addressed at the level of *“an individual,”* [18] digital security is a social, interpersonal, and community issue. They maintained further that some of the most effective measures to build awareness and protect people from harm arise in a social or community setting and emphasized the need for institutions—not just internet users, individuals, or policy beneficiaries—to review and update protocols and practices in view of increased risk.

They stressed that while interventions such as digital hygiene trainings are critical, many broader risks and harms will not be addressed through training alone. Digital hygiene includes education in topics such as strong passwords, two-factor authentication, cookie settings, application downloads and updates, public and private social media settings, and some awareness of what phishing and other forms of fraud look like. However, such training cannot address sophisticated fraud and ransomware operations, nor can it address ways in which communities learn and develop norms around how they use internet-enabled technologies collectively to reduce risk.

"It's not that training isn't the answer," says Daniel Kahn Gillmor, senior staff technologist for the ACLU. "It's reasonable to say that we want to give people hints and tools, but if we shift the burden to the individual, then we've failed to address the underlying, systemic problems." Seeta Peña Gangadharan puts it this way:

> "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 on an ongoing basis, then we're missing the point."

Interviewees pointed out that expectations placed on individuals to become sole guardians of their safety online are even more unreasonable given basic digital literacy struggles for new internet adopters.

State digital equity plans across the country provide clear consensus that basic skills—including video chatting, storing and finding files, and even using email—can be challenging for late adopters, let alone toggling privacy settings or using a virtual private network (VPN). This is particularly true for new and infrequent users who mostly access the internet from public facilities.

"If you don't use your email that often—you use it once in a while at the library [...]—then people will tend to fall for phishing scams more. People lose money. They get their identities stolen," says Myeong Hong Hurwitz, founder of digital security service provider Tiny Gigantic.

Gangadharan points out further that even when people do successfully acquire basic digital skills, the burden of self-protection is still unrealistic:

> "Plenty of people help themselves to working around data-driven systems. However, when something goes wrong, there are very few people to turn to or institutional frameworks to rely on. Whether it's identity fraud, theft, or expungement [removing harmful or inaccurate data trails and profiling], people are going to hit a wall... or a really unhelpful, impenetrable chatbot that claims to be about customer service."

Hong Hurwitz also notes 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.”

Leigh Honeywell, CEO of digital safety provider Tall Poppy, adds that “people are targeted because of their jobs and where they work. The companies that hire employees have a duty of care to protect the people that work for them, in the same way that they need to fulfill occupational health and safety requirements.” Both Hong Hurwitz and Honeywell explain that organizations that represent traditionally marginalized groups, and those that are targeted for political reasons, experience a higher level of threat than others.

Along with virtually all other interviewees, Hong Hurwitz and Honeywell stress that the implications of placing the burden of safety on the most vulnerable internet users presents a broader threat to our society. Tawana Petty—Just Tech Fellow, longtime Detroit organizer, and founder of multiple digital safety initiatives—adds:

> “There’s also a psychological element. When communities start to realize the threats that exist, it is demoralizing and creates anxiety. People get paralyzed; they don’t know what to do. While tech is everywhere, we are just learning about new problems that arise with it. People don’t know where to start. It’s your phone; it’s software—how do you know what to trust? What do you do if you feel under threat?”

## 2. ACCOUNT for DIFFERENT EXPERIENCES of TECHNOLOGY, INCLUDING HARM, SURVEILLANCE, and PREDATION

Those who work every day with victims of digital harm cite increased threats and risk especially for new and traditionally marginalized populations. Tawana Petty explains that aging individuals, Black and Brown communities, new and less practiced internet users, limited English speakers, people living with disabilities, veterans, and other less connected groups (including many of the Covered Populations defined in the Digital Equity Act) 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 is being contained in surveillance tech mechanisms,” says Petty. Methods can include warrantless data collection and algorithmically driven policing, which disproportionately use the data trails of criminalized populations to monitor and predict activity. Una Lee, founder of the Consentful Tech Project, contends that “the folks who are weaponizing this technology are using it against those who have less power—for example, white and rich folks surveilling their Black and Brown neighbors.” Aki Younge, director of movement collaborations for the UCLA Center on Race & Digital Justice, adds that “the folks that are the most vulnerable to getting targeted for fraud, especially an exploitative kind of fraud, are folks of color; and the folks that are most likely to get hacked online are people who have things that they want to say about power and oppression.”

Both Leigh Honeywell and Myeong Hong Hurwitz also warn about explicitly racist and antisocial activity on the internet targeting traditionally marginalized groups, explaining that many of their clients come to them after being targeted based on racial identity, ethnicity, gender, and other political and social markers of difference. Younge points out that this dynamic, as well as awareness of the mechanics of data harvesting by institutions of the state or data brokers for surveillance, has a curtailing effect and prevents people from trusting the internet at all. “When you know how much of this information is being collected on you, it has this chilling effect,” she says. “If you are someone who is vulnerable in any way, the more connected you are to the digital world, the more leakage of your information happens. That makes it a higher risk to not only do the daily things you do but to say something against an entity of power.”

Younge also notes that given the vulnerability of large computer systems to hacking and fraud, participation in digital inclusion activities can open the DEA’s Covered Populations up to risk when their information is held in large databases:

> “If you are someone who applies for benefits online through a portal, that information is making you vulnerable. If you are someone who’s applying for the Affordable Connectivity Program, you have given personal information to the internet service provider company, and that’s an axis of vulnerability for you as well.”

For these communities, password trainings or cybersecurity apps are woefully insufficient to address the range of risks and harms they are facing. Many of our interviewees argue that the best approach is to support communities in assessing and understanding their risk profile and to develop collective, culturally relevant strategies. Myeong Hong Hurwitz says:

> "Successful cybersecurity precaution looks like a group of people doing an assessment of what kind of cybersecurity they need and making a plan. They'd need support in implementing that plan and support with incident response. They'd need support in having ongoing conversations about privacy and cybersecurity."

Our interviewees also stress that those designing and implementing programs to improve digital safety for historically marginalized communities should have a deep understanding of the range of threats they face. In fact, given deep distrust between traditionally marginalized groups and government, our interviewees contend that it is critical to support and build talent from within the communities who are most impacted, rather than bringing it in from outside. "We have to invest in diverse tech talent, so that the people offering help are from those communities and understand their challenges. People from vulnerable communities should be upskilled to do audits and fixes," says Daniel Kahn Gillmor of the ACLU.

## 3. DESIGN HOLISTICALLY for COLLECTIVE RISKS and UNDERSTAND BROADER SOCIETAL IMPACT

While some digital harms may emerge from individuals' online behaviors—or may be addressed with virus protection or privacy-protecting apps—policymakers, legislators, and practitioners have more work to do to truly grapple with the range and global expanse of digital risks opened up by data-driven technologies.

As described above, virtually all interviewees expressed that vulnerable communities, who are often more integrated into complex social benefits systems, and who are surveilled at a higher rate by law enforcement and social service providers, also have a higher threat profile due to the amount of personally identifiable information and records that are stored in government databases. These threats may come from both state and non-state actors.

Sandra Ordóñez, head of team at Team CommUNITY and a global digital rights leader, explains that consolidation of data on the internet creates massive efficiencies of scale for fraud due to the sensitive information sitting in databases with various levels of protection.

> “Efficiencies of scale favor bad actors—and the internet is a key driver for efficiencies of scale. 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.”

Leigh Honeywell points out that “we are in a moment of the industrialization of scammers and fraud coming from overseas, targeting people in the states at the peak of their net worth, right before they retire.” Industrial scammers can use personal information bought and sold by data brokers, or sitting around in various databases, to trick targets into engaging in extended interaction and eventually depleting their life savings based on a story fabricated from real details of a person’s life. Honeywell warns, “We are going to face a substantial social problem of people who would have otherwise been self-sufficient, but lose their life savings to fraud, if we don’t educate everybody in the stack, from the individuals to their financial institutions.”

Daniel Kahn Gillmor agrees:

> “Government actors at various levels share information with each other. Similarly, a non-state actor like a criminal gang or a foreign adversary [is] going to see pots of data out there as attractive targets. If we have a pool of money in our banks, we should invest in institutions that are dedicated to reducing the digital footprint of vulnerable people, or the destructive effect could be at massive scale.”

Both Gillmor and Ordóñez emphasize the increasing threat to all American residents based on the attractiveness of vulnerable communities’ data, and the specific risk of predation for new and less digitally skilled internet adopters. Bringing vulnerable communities online without taking steps to address the weaknesses of data systems creates vulnerability for our full financial system—and even GDP.

The Digital Equity Act, with the necessary goal of ensuring equal access to the means of participation in our cultural and social systems, must not place the burden of safety on its beneficiaries. Otherwise, all of us will experience the effects—but the harms will disproportionately, again, fall upon those who can bear them the least.

# HOW STATES ARE DESIGNING FOR DIGITAL SAFETY

## PRIVACY and CYBERSECURITY in the BIPARTISAN INFRASTRUCTURE ACT and STATE DIGITAL EQUITY PLANS

While awareness and use of tools to protect cybersecurity and data privacy are included in the Digital Equity Act's Measurable Objectives, it is a relatively new area of inquiry for digital inclusion.

The National Telecommunications and Information Administration (NTIA) encouraged all states to gather data on the five measurable objectives listed in the Digital Equity Act (including Objective 4, Cybersecurity),[19] and each state applied its own research questions, methodologies, and survey and focus group instruments to determine the nature and impact of safety and privacy risks for its residents. The following audit of state plans shows a range of analyses, problem identifications, and possible solutions. Overall, the data show that the vast majority of U.S. residents express strong concern about digital privacy, security, and safety; beyond that, the particular risks and solutions vary widely.

## STATE PLAN HIGHLIGHTS on SAFETY, SECURITY, and PRIVACY

- Over 40 percent of **Californians** surveyed cited concerns over privacy as a barrier to accessing home internet.
- In **Idaho**, "Cybersecurity was mentioned as a concern in 100 percent of focus groups. The state found a broad range of privacy awareness levels, from residents who trust in anything and anyone they encounter online to those who refuse to use a device at all out of fear that being connected to the internet is too dangerous."

- In **Maine**, 93 percent of survey respondents were concerned about internet safety. “In focus groups and community meetings, people almost universally expressed concern about hacks and scams, their ability to protect their data and privacy online, and older family members and children staying safe online.”
- In **Minnesota**, people who have experienced cybersecurity threats or who have close friends or family who have been harmed by scams may be keenly distrustful of low-cost programs that seem “too good to be true.”
- **New York** found that 87 percent of residents surveyed were either somewhat concerned or very concerned about their online safety, including 92 percent of aging individuals (60 and above). “Focus groups across the state indicated a range of concerns including online scams and fraud, hate and harassment, misuse and theft of data, and surveillance and discrimination. Participants articulated that ‘all of it is overwhelming and leads towards a general “technophobia” when it comes to using the internet at all.’”
- **Utah** found that “search engines and targeted ads may discriminate against individuals with a language barrier by not providing them with relevant or accurate information, or by providing them with lower-quality or less relevant ads.”

## OVERALL QUANTITATIVE SECURITY and PRIVACY RISK FINDINGS by STATE

| | |
|---|---|
| **ALABAMA** | 5.4% of all households that do not use the internet at home cited online security or privacy concerns as a reason. In the past year, 15.5% of individuals in Covered Populations report having been the victim of an online security or privacy breach. |
| **ALASKA** | 56% of residents surveyed expressed "Concerns about Online Safety/Privacy." |
| **CALIFORNIA** | 42% of Californians cited concerns over privacy as a barrier to home internet. About a quarter of all online public survey respondents said they were unfamiliar with cybersecurity measures. |
| **COLORADO** | For immigrants responding to the Statewide Digital Equity Survey, 56% were unfamiliar with measures needed to stay safe online or didn't know what cybersecurity meant. Listening sessions with communities across Colorado revealed that those with language barriers feel particularly vulnerable to cybersecurity threats. Some shared that they felt immigrants establishing their life in the United States are targets for scam attempts, yet instructions on how to protect themselves online are typically in English only. |
| **GEORGIA** | In the past year, 13.1% of individuals in Covered Populations in Georgia reported having been the victim of an online security or privacy breach. Identity theft and credit card fraud were the two online security risks that concerned the most Georgia residents. Among the specific Covered Populations, people with disabilities, veterans, and individuals at or above 60 years of age tended to be the most concerned about these risks. |
| **IDAHO** | Cybersecurity was mentioned as a concern in 100% of focus groups. |
| **MAINE** | 93% of survey respondents were concerned about internet safety (50% very concerned), focusing on effectively protecting older adults and children. In focus groups and community meetings, people almost universally expressed concern about hacks and scams, their ability to protect their data and privacy online, and older family members and children staying safe online. |
| **MASSACHUSETTS** | Residents from all backgrounds and regions reported concerns about internet safety, with 85% of survey respondents statewide citing this concern. Aging individuals across the state were highly concerned with internet safety, specifically citing concerns about online scams or online hacking. Individuals with a language barrier were least likely to be aware of resources to protect their safety online. Individuals with disabilities highlighted concerns about medical data breaches. Residents expressed concerns about youth safety online. |

| | |
|---|---|
| **MONTANA** | 15% of survey responses indicated that people don’t have internet at home due to privacy or cybersecurity concerns. |
| **NEW MEXICO** | 17.8% of individuals in Covered Populations reported having been the victim of an online security or privacy breach. |
| **NORTH CAROLINA** | Survey respondents did not feel particularly confident in their ability to protect themselves online, with 42% feeling very confident in their ability to keep themselves safe online and 36% in protecting their personal data. This issue was also brought up multiple times during the listening sessions. Many residents were concerned about online scams and expressed a desire for more services and support for cybersecurity and privacy training. |
| **PENNSYLVANIA** | Among aging populations, high costs (29%), unreliability (23%), and security and privacy concerns (18%) were the most frequently cited challenges to internet access. Among minorities, high costs (53%) unreliability (27%), and security and privacy concerns (23%) were the most frequently cited challenges. Among veterans, high costs (8%), unreliability (7%), and security/privacy concerns (5%) were the most frequently cited challenges. |
| **VIRGINIA** | Research has indicated that refugee populations are at heightened risk of cyber vulnerability due to a lack of awareness of cybersecurity measures or because they are using the internet to stay in touch with family and friends who may be in regions with limited data privacy and protection; these same vulnerabilities can be understood as true for English-learning refugee populations in Virginia, as well as further extrapolated to the broader English-learning community, who already experience heightened vulnerability to scams posing as resources. |
| **WASHINGTON, DC** | DC Broadband Access and Digital Equity survey respondents… worry about their digital safety at least once a week. 31% of respondents specifically expressed concern regarding the privacy and security of their personal data; 23% expressed concern about online fraud and phishing. |

NOTE: Many states included only high-level, general, or summative comments regarding the current state of digital security and safety, without qualitative or specific findings.

# COMMON DIGITAL SAFETY and SECURITY MEASURES CONTEMPLATED by STATES and TERRITORIES

## PUBLIC-FACING PROGRAMS

Digital Safety and Security Campaigns (AL, DC, IA, ID, ME, and others)

CBO and CAI-based security training, including libraries (DE, FL, MD, ME, MN, NC, OH, OK, OR)

Privacy and safety information resource provision (NM, OK, and others)

Physical tech hubs providing safety and security support (DC)

Trainings, including Digital Navigator–led (many); PPP bootcamps (GA); digital hygiene (PA); digital citizenship in schools (TN, UT)

Cybersecurity inclusion in digital literacy training (VT)

## DEVICE-BASED TOOLS

Free antivirus software, apps, and other tech tools and resources (DC, KY, ND, UT)

Provision of tools and resources such as how to recognize and report online scams (DC)

## WORKFORCE/PIPELINE PROGRAMS

Development of security-focused Digital Navigator corps (MS)

Alignment with state cybersecurity centers/law enforcement job pipelines (GA, KY, LA, ND)

Cybersecurity career and workforce opportunities (SC and more)

Google career and other certificates through Digital Navigators partnerships (IA, WV)

## PROCUREMENT and GRANTMAKING

Partnerships with ISPs with the expectation that ISPs increase cybersecurity standards including ensuring that covered populations are protected online through threat monitoring, firewall features, and reporting suspicious activity across ISP networks (DC)

Ensure that subrecipients adopt NIST cybersecurity framework (WY)

Prioritize funding requests that integrate safety/privacy (NH)

Full integration into state subgrant digital skills programs (RI, NV, NJ)

## DIGITAL SAFETY and SECURITY SCORING METHODS

Score is a calculation of percentage of each Covered Population that has refrained from one or more online activities due to cybersecurity concerns; or who do not use the internet at all based on such concerns. Proposed KPIs measure effectiveness of communications strategies; examples of good cyber-hygiene to model behavior; coordination with Digital Navigator programs; and intergovernmental coordination (MI).

Digital Connection, Digital Literacy, and Digital Security benchmarks for all residents and members of each Covered Population. The order is based on the Digital Connection Benchmark Score, based on U.S. Census data (CT).

# RECOMMENDATIONS

States and territories responsible for Digital Equity Act Capacity Grant allocations are charged with creating programs to address data privacy and cybersecurity for Covered Populations, and with tracking the progress of those efforts. The information in this report points to critical considerations for administering entities in view of the breadth, range, and variety of risk vectors for new, vulnerable, and traditionally marginalized groups.

Capacity Grant administrators can leverage their oversight and strategic management of grant-funded programs to create best outcomes for Covered Populations and others most at risk for harms including harassment, fraud, targeting, and data theft. Administering Entities can also develop pipeline and workforce programs that tap into the lived expertise of the most-impacted communities to expand capacity and develop culturally appropriate materials and support systems. States and territories can also deploy procurement rules and standards to address broader systemic and institutional risks. Finally, administering entities can develop evaluative key performance indicators (KPIs) that keep programs and implementation on track to deliver improved safety and security outcomes.

We have grouped our recommendations into four areas that braid together the emergent digital safety measures contemplated by states and territories and the specific recommendations and expertise of the cybersecurity, privacy, and safety leaders we consulted to develop this report:

## 1. Program Design Principles

*Establish Tenets for building DEA Capacity and Competitive Grant training programs and campaigns such as those identified by our audit of State Digital Equity Plans.*

Invest in holistic and culturally aware training and community support solutions:

- Shift the perspective from burden on the individual to collective culture-building and support;
- Hold digital hygiene trainings at libraries and other public computing centers familiar to those who are most impacted by digital harms;
- Provide culturally competent learning atmospheres and curricula;
- Provide community risk assessment and strategic digital safety planning programs, not just programs to train individuals on digital hygiene;
- Go beyond mechanics like password basics to address social media norms and settings, recognizing targeted fraud and reducing embarrassment or shame to encourage people to discuss and build safety circles with friends and family; and
- Build digital safety across grant programs to ensure safety across a range of digital skills and internet uses—for example, accessing social services, adjusting security settings on newly acquired devices and applications, using public Wi-Fi, and when participating in civic activity or accessing health care.

## 2. Workforce, Pipeline, and Capacity Development Programs

*To expand the range of informed and culturally relevant safety support resources available, invest in and support training and employment of safety experts from Covered Populations and other vulnerable groups.*

- Invest in diverse tech talent, including scholarships prioritizing applications from most-impacted populations, including Covered Populations;
- Design workforce development programs to prioritize training and placement for members of Covered Populations in privacy and cybersecurity positions;
- Fund intermediaries from within communities to conduct audits, risk assessments, bug reporting, monitoring, safety support provision, and support for device maintenance and software updates. This can be an adapted Digital Navigator role with placement at existing organizations.

# 3. Procurement and Grantmaking Standards

*Administering Entities have a duty of care to protect beneficiaries as well as organizational subawardees in DEA-funded programs and activities. Implementing DEA programs themselves will involve many risk vectors, including the security of devices, software, and databases. Administering Entities may adopt standards governing these factors and pass them down to contractors and prospective grantees. Suggested standards and requirements include:*

## RISK ASSESSMENTS

- Create interagency agreements and grantmaking instruments (RFP, RFI) that require a risk assessment as part of the contracting process, with mitigation strategies a requirement of contract execution; and
- Require state-level review of public-facing grant-funded systems and devices from Domain Name Systems (DNS) to hardware.

## DEVICE and SOFTWARE STANDARDS

- Prohibit administrative "back doors" and other spyware in program-distributed devices;
- Ensure that distributed devices have sufficient processing speeds and maintenance requirements to allow for software updates; and
- Consider a policy for software auto-updates.

## DATA POLICIES

- Create a policy governing data collection by third parties on hotspots and other networked devices distributed with grant funds;
- Anonymize Personally Identifiabe Information (PII) in program records except where strictly necessary, and expunge all PII after a specific time period; and
- Prohibit unnecessary data collection.

### APPS and VIRUS PROTECTION

- Create standards for data collection by apps and third-party tools distributed to the public;
- Conduct regular audits on automated tools; and
- Prohibit user monitoring on devices with DEA-funded tools and software installed.

### ARTIFICIAL INTELLIGENCE

- Create principles around the use of artificial intelligence in grant programs—for example, the White House Office of Science and Technology Policy AI Bill of Rights.

## 4. Evaluation and Scoring

As shown in the audit of state and territory assessments of digital safety and security above, available research methods to gauge safety and security among a population are often a reflection of sentiment—that is, the feeling that people have about safety or lack thereof. As U.S. states and territories rapidly compile digital equity data and Digital Equity Act programs mature, we have a critical opportunity to develop scoring and impact metrics in this category of digital equity barriers.

Connecticut and Michigan have provided model frameworks to set a baseline and measure progress toward greater digital safety, and Wyoming is leveraging the National Institute of Standards and Technology's cybersecurity framework. We encourage states to conduct additional research to illuminate the kinds of measures that succeed over time in reducing feelings of insecurity and risk that discourage adoption and use of the internet.

# CONCLUSION: The Imperative to Address Digital Risk in Pursuing Digital Equity

The findings and recommendations captured in this report point toward the need for more research and due diligence on the impact of digital harms on new and vulnerable internet users, as well as the development of standards around protecting these groups alongside future digital equity activities. We recommend that policymakers, officials, and practitioners learn with and from those who are experiencing the most harm and codesign programs with them, along with prioritizing those groups' leadership and employment within safety and security fields.

Amid an unprecedented effort to expand connectivity and adoption, it is imperative to ensure that those entering the digital world are meaningfully protected from the internet's downside. For broader impact on sustainability and on areas affected by meaningful internet adoption, such as health care, education, and workforce development, the DEA's public funding opportunity should be supplemented with catalytic investments from philanthropy and the private sector. Along with the public sector, philanthropy has an opportunity right now to invest in effective programs to build future-ready safety awareness, tools, and practices.

If this opportunity is not considered carefully, the DEA's unprecedented expansion of digital access could also, paradoxically, open its beneficiaries up to unprecedented risk and harm, and could even weaken the defenses of all of the country's digital and financial systems.

Of course, implementation of Digital Equity Act programs cannot solve all the complex problems involved with perverse incentives and economies of scale that are a part of our increasingly data-driven world. There is a need for policymakers as well as public and private institutions to align on a clear analysis and approach to the larger issues. Problems of digital risk, fraud, abuse, mental health impact, disproportionate application of unregulated algorithmic tools, and more are rightfully the targets of the Federal Communications Commission, the Federal Trade Commission, the National Institutes of Health, and all other departments of government and bodies tasked with protecting the public interest.

And yet the way that federally funded broadband programs, including the Digital Equity Act, take shape will become a determining factor in how the United States as a country considers and values internet participation. We want the benefits of broadband to reach everyone, and we want everyone to have a voice in our economy, society, and democracy—but if participation brings harm, then the promise of ***internet for all*** is betrayed, and a democratizing force can become an oppressive one.

This report is intended to create awareness around the need for safety while also protecting the values of the free and open internet, which enables members of marginalized communities to find one another, find common ground, and make their voices heard. Our aim is not to undermine or limit access to critical technologies in any form but rather to build norms and systems that enable communities and individuals to protect themselves while also participating in thriving digital worlds.

For many digital equity experts and practitioners, the primary problem to be solved by investing in cybersecurity and privacy measures is to reduce the likelihood that fears about safety become barriers to adoption. But the risk of not sufficiently guarding against harm to new and vulnerable internet users is existential for the field.

We can address this paradox through a shared intention to imagine future connected technologies that fit not only who we are but who we aspire to be. To get there requires an honest examination of the assumption that internet access is by default and on its own a social good. As always, creating healthy media and technology environments requires constant, critical observation and analysis—and a commitment to listen most closely to those who have been left out and unprotected.

# APPENDICES

## Appendix 1: SAMPLE of DIGITAL SAFETY RESOURCES

### The Tech Worker Handbook

**Matt Mitchell**

The Tech Worker Handbook is a collection of resources for tech workers who are looking to make more-informed decisions about whether to speak out on issues that are in the public interest. Aiming to improve working conditions, direct attention to consumer harms, or otherwise address wrongdoing and abuse should not be a solo or poorly resourced endeavor.

In this guide, Matt Mitchell and the experts of Elite Strategy Global cover a range of information and physical security concerns that all tech workers should be aware of—whether or not they ever consider whistleblowing.

### PRIVACY RECIPE: Creating an Online Persona

**Matt Mitchell/Crypto Harlem**

This article explains how to create a private online identity with an anonymous email address and a virtual phone.

### Digital Defense Playbook

**Our Data Bodies**

Our Data Bodies (ODB) has conducted research and produced a workbook of popular education activities focused on data, surveillance, and community safety to cocreate and share knowledge, analyses, and tools for data justice and data access for equity. We hope that our work will enhance trusted models of community health and safety and help illuminate the differences between being safe and being secure.

### Surveillance Self-Defense

**Electronic Frontier Foundation**

Surveillance Self-Defense (SSD) is a guide to protecting yourself from electronic surveillance for people all over the world. Some aspects of this guide will be useful to people with very little technical knowledge, while others are aimed at an audience with considerable technical expertise and privacy/security trainers. We believe that everyone's threat model is unique—from activists in China to journalists in Europe to the LGBTQ community in Uganda. We believe that everyone has something to protect, whether it's from the government or parents or prying employers, stalkers, data-mining corporations, or an abusive partner.

### A First Look at Digital Security

2018 (Updated 2023)

**Access Now**

We created "A First Look at Digital Security"—an open-source booklet—to help you take the first steps toward improving your digital security online, and we continue to update it online at GitLab to make sure it remains accessible for anyone who needs it. The guide uses five user archetypes to introduce the concept of threat modeling, and there is a glossary to explain the most difficult terms and ideas. If you are a digital security trainer, you can use and further develop the user archetypes that we present as scenarios for your teaching activities, and we have now added space—a blank persona-building page—that your students can use to create their own threat model, based concretely on their particular situation and needs.

### A First Look at Digital Security: Glossary

2019 (Updated 2023)

**Access Now**

This is a glossary of terms that can be found in the A First Look at Digital Security booklet.

### Signal for Beginners

2016 (Updated 2023)

**Martin Shelton**

Signal gives you encrypted messages, as well as voice and video calls. It relies on data, so it's a great option for free calls and texts over Wi-Fi. This can be a huge advantage for those who don't want to pay for SMS text messages and phone calls, or who want to make free international calls.

### Precisely Private Good Privacy Practices

2017 (Updated 2024)

**Tobia Alberti**

This is an online privacy guide for the general public. It's composed of a list of widely recognized best practices everyone should consider adopting in order to better protect their privacy and security online.

### Digital First Aid Kit

2019

The Digital First Aid Kit is a free resource to help rapid responders, digital security trainers, and tech-savvy activists to better protect themselves and the communities they support against the most common types of digital emergencies. It can also be used by activists, human rights defenders, bloggers, journalists, or media activists who want to learn more about how they can protect themselves and support others. If you or someone you are assisting is experiencing a digital emergency, the Digital First Aid Kit will guide you in diagnosing the issues you are facing, and refer you to support providers for further help if needed.

### Defend Our Movements

2018

**MediaJustice**

This is an online, collaborative source of questions/answers, resources, links and other information about protecting your data—brought to you by MediaJustice, May First Movement Technology, and diverse movement technologists and activists.

### Data Dictionary and Controlled Vocabulary

Updated 2020

**Berkeley Copwatch Database**

**WITNESS**

This Data Dictionary + Controlled Vocabulary was created for Berkeley Copwatch's People's Database for Police Accountability. It defines the fields used in the database and the rules for entering data, including lists of terms and their meanings. It serves as a reference for Berkeley Copwatch to ensure consistent cataloging and accurate interpretation of the data.

### NYC Digital Safety: Privacy and Security

2022

**Brooklyn Public Library**

Brooklyn Public Library created training and resources for public library staff.

# Appendix 2:
# INTERVIEW SCRIPT

Thank you for taking the time to speak with me today.

The purpose of this conversation is to inform decision-makers about individual and community needs for digital privacy, security, and safety support and training in the context of unprecedented levels of investment in internet access and literacy under the Infrastructure Investment and Jobs Act of 2022. We are hoping to hear from you about what you have learned in your work with individuals and communities: their concerns, experiences, and hopes regarding safety, security, and well-being online.

Please note that your participation in this interview is voluntary. You may choose not to answer any of the following questions, and we can stop the interview at any time.

Would you like to proceed with the interview? (verbal consent)

1. In a couple of sentences, could you describe the online privacy, security, and safety training and preparedness work you do?

    a. Who is it directed toward and why?

2. If you had to pick one or two threats to prepare for, which of these do you think is most important to the people you work with?

    a. Data privacy

    b. Protection against fraud or hacking

    c. Online harassment or threats

    d. Surveillance and discrimination

    e. Something else

3. From your experience working with specific community groups, what should government officials know about what's at stake if internet security and safety concerns are not addressed?
    a. Can you share some anecdotes?
    b. What are the vulnerabilities? Who's more vulnerable than whom?
    c. Who represents a threat and why/how?
        i. Corporate?
        ii. State?
        iii. Non-state actors?
4. What does successful privacy and cybersecurity preparation look like?
5. What support do you need to do your work successfully and at scale?
6. What sources/resources would you recommend to use to familiarize ourselves with cybersecurity and privacy preparation?
7. Who else is doing this work that we should know about?

# ENDNOTES

[1] ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public

[2] thecut.com/article/amazon-scam-call-ftc-arrest-warrants.html

[3] fcc.gov/document/fcc-oig-announces-acp-provider-repaid-nearly-50m-issues-advisory

fcc.gov/document/fcc-proposes-14m-fine-and-initiates-removal-acp-violations

lexology.com/library/detail.aspx?g=c51cb368-a5e0-4e45-9997-8ba229ebd1c6

topclassactions.com/military-government-political/unnamed-internet-provider-repays-fcc-49m-for-improper-subsidy-claims/

fiercewireless.com/wireless/fcc-proposes-fine-q-link-wireless-62m-related-acp

[4] ftc.gov/system/files/documents/reports/serving-communities-color-staff-report-federal-trade-commissions-efforts-address-fraud-consumer/ftc-communities-color-report_oct_2021-508-v2.pdf

[5] pewresearch.org/internet/2023/10/18/how-americans-protect-their-online-data/

[6] pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/

[7] pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/

[8] nationalfairhousing.org/resource/privacy-technology-and-fair-housing-a-case-for-corporate-and-regulatory-action/; https://link.springer.com/article/10.1007/s10506-021-09286-4

[9] naacp.org/resources/artificial-intelligence-predictive-policing-issue-brief

[10] cbsnews.com/news/health-insurance-humana-united-health-ai-algorithm/

[11] Seeta Peña Gangadharan, “The Downside of Digital Inclusion: Expectations and Experiences of Privacy and Surveillance among Marginal Internet Users” New Media and Society 19, no. 4 (April): 597–615

[12] David Barnard-Wills, “E-Safety Education: Young People, Surveillance and Responsibility,” Criminology and Criminal Justice 12, no. 3 (July 1, 2012): 239–55.

[13] Safiya Umoja Noble, Algorithms of Oppression: How Search Engines Reinforce Racism (New York: New York University Press, 2018)

[14] Ruha Benjamin, Race after technology: Abolitionist tools for the new Jim code (Polity, 2019)

[15] Virginia Eubanks, Digital Dead End: Fighting for Social Justice in the Information Age (Cambridge, MA: MIT Press, 2011)

[16] Wilneida Negrón, “Little Tech Is Coming for Workers: A Framework for Reclaiming and Building Worker Power,” CoWorker (2012)

[17] Lewis, T., Gangadharan, S. P., Saba, M., Petty, T. (2018). Digital defense playbook: Community power tools for reclaiming data. Detroit: Our Data Bodies.

[18] (“awareness of, and use of, measures to secure the online privacy of, and cybersecurity with respect to, an individual”)

[19] “Measurable Objective” categories as listed in statute [47 U.S. Code § 1723]

- Access to affordable broadband service
- Access to devices that meet the needs of users, and support for those devices
- Access to digital literacy and skills training
- Awareness and the use of measures to secure the online privacy of, and cybersecurity with respect to, an individual
- Accessibility of online government and essential services

# AUTHOR

**Greta Byrum** is a 2023-2024 Marjorie & Charles Benton Opportunity Fund Fellow.

As a leader in digital equity and community wireless networking, Greta has worked in digital equity and internet policy since 2011. For seven years, she led tech policy and community engagement projects at New America as director of the resilient communities program and director of field operations for the Open Technology Institute. She built Resilient Networks at New America, a $4 million post-Hurricane Sandy partnership with the New York City Economic Development Corporation, the Department of Housing and Urban Development, philanthropic organizations, and community-based organizations.

Greta went on to found Community Tech NY, a nonprofit working with community digital stewards to build storm-resilient community Wi-Fi in New York City, Detroit, and rural Tennessee. She co-founded and built the Digital Equity Lab at the New School with civil rights leader Maya Wiley; and set up and launched the $12 million Just Tech Program for the Social Science Research Council, a fellowship and platform dedicated to imagining and creating more just and equitable technological futures.

Greta currently serves as a principal for HR&A Advisors with a focus on broadband, digital equity, and emerging technologies.

BENTON INSTITUTE for BROADBAND & SOCIETY

Broadband Delivers Opportunities
and Strengthens Communities