DATA&
SOCIETY

January 14, 2022

Request for Information on Public and Private Sector Uses of Biometric Technologies

Dear Dr. Eric Lander and Dr. Alondra Nelson,

Data & Society Research Institute is pleased to submit a response to the Request for Information (RFI) published by the Office of Science and Technology Policy (OSTP) on past deployments and current use of biometric technologies in the public sector.

Our organization is an independent, nonprofit research institute studying the social implications of data-centric technologies and automation. We are working to help ensure that artificial intelligence (AI) systems are accountable to the communities within which they are applied, and to produce empirical research that challenges the power asymmetries created and amplified by technology in society. We have worked extensively with civil society and advocacy communities, and in solidarity with marginalized communities and workers directly affected by algorithmic harms.

We are pleased to see the OSTP's commitment to create a Bill of Rights for an Automated Society and to ensure new and emerging data-driven technologies abide by democratic values.[1] It is essential that we develop AI policy and governance mechanisms responsive to the prevalence of AI systems that enable discriminatory practices and that expose marginalized communities to harm.

In this comment, we highlight the biometric surveillance of care workers and care recipients through electronic visit verification (EVV) systems, in order to encourage OSTP to explore how the public sector adoption of biometric technology has ignored the needs of marginalized communities and has led to tangible harm. By centering the harms generated by the growing landscape of punitive technologies that target and criminalize both low-wage workers and public benefits recipients, OSTP can ensure that the government commits to community- and justice-informed uses of algorithmic systems.

In this comment, we recommend that OSTP:

- **Support federal agencies in their efforts to better understand the use of automated systems in public benefits delivery, and ultimately recommend the**

[1] https://www.whitehouse.gov/ostp/news-updates/2021/11/10/join-the-effort-to-create-a-bill-of-rights-for-an-automated-society/

prohibition of technology that further marginalizes and harms the communities who are entitled to benefits and care.

- **Commit to research and policy proposals that center community and justice-informed uses of algorithmic systems.**

1. Electronic Visit Verification Systems & Biometric Surveillance *(Questions 1, 4)*

Emerging harms from uncritical public sector adoption of algorithmic technology

Public institutions are increasingly turning to technical fixes to solve structural problems, and consequently, sidelining questions of inequality, accountability, and justice. **Within public benefits programs, federal and state governments are introducing algorithmic technologies like EVV to police vulnerable communities under the guise of rooting out fraud, waste and abuse, rather than passing and implementing policy in consultation with those communities and in response to their needs.** These technologies introduce automated, algorithmic processes that lack transparency and mechanisms for appeal, putting the onus on vulnerable individuals with scarce resources to not only push back, but to advocate for services and benefits they have a right to expect from the state.

As the largest single funder of long-term services and supports, the United States government—through programs like Medicaid—plays a significant role in providing necessary care and support services for people with disabilities and older adults. As a result, greater public sector use of technology is impacting both the care workforce and the families they support. Just as the use of automated systems in areas like education, criminal justice, and welfare have already led to deeply inequitable outcomes, the adoption of these technologies in Medicaid home- and community-based programs may perpetuate extractive and punitive approaches towards managing, quantifying, and distributing care across our society.

Our recent research report, "Electronic Visit Verification: The Weight of Surveillance and the Fracturing of Care,"[2] finds that the surveillance of US home care workers through a state-funded EVV mobile apps erodes critical support for people with disabilities and older adults while offloading significant, unacknowledged burdens onto both workers and service recipients within Medicaid home- and community-based services. The implementation of EVV systems highlights the risks of uncritical adoption of data-centric and biometric technologies in the provision of public services.

[2] https://datasociety.net/library/electronic-visit-verification-the-weight-of-surveillance-and-the-fracturing-of-care/

Biometric Surveillance of Care Workers and Care Recipients

Congress passed the 21st Century CURES Act in 2016, which included a provision that required all Medicaid-funded personal care and home health care services to use EVV systems. EVV systems are a form of digital workplace monitoring that tracks homecare workers' time, location, and other data in order to confirm that services were delivered.

While EVV systems may seem to be just another digital timekeeping tool and method for ensuring quality of care, these systems were federally mandated to serve wider policy ambitions to reduce "fraud, waste, and abuse" in publicly-funded personal care and home health services. However, rather than producing an accurate measurement of fraud, waste, and abuse, EVV systems routinely flag workers for minor errors and glitches. **Although the federal legislation that mandated EVV required the systems to be "minimally burdensome," in practice, little federal policy guidance was provided on how to adhere to this goal, resulting in deeply invasive data collection being encoded into state policies and technology design, including GPS location tracking, geofencing, and biometric data collection like facial and voice recognition.**

EVV systems use GPS location tracking, geofencing, and biometric data collection to track workers and, by extension, their clients. Rigid policies and biometric technology requirements that pressure individuals to comply with strict program rules have had a chilling effect on service recipients' lives and has made workers' jobs more difficult. Home- and community-based services are essential and life-sustaining for Medicaid service recipients, which means they have no choice but to opt into data collection through EVV systems as a condition of receiving services. Service recipients and workers spoke of feeling criminalized, viewing EVV as an extension of broader legacies of government surveillance over people of color, and poor, disabled, and older adults.

These GPS and biometric features have been some of the most contested aspects of the EVV mandate. Advocacy groups have particularly focused on banning the use of GPS tracking and biometric data collection on a national level,[3] and their use has also contributed to privacy backlash from disability communities at the state level.[4]

- **Facial Recognition**: Facial recognition is commonly implemented within EVV platforms for the purpose of identity verification, which seeks to match a photograph taken by the worker to a photo kept on file. Typically, a worker is required to

[3] https://www.foley.com/en/insights/publications/2020/05/century-cures-act-personalized-medicine-covid-19

[4] https://coloradosun.com/2019/12/23/evv-requirement-for-medicaid/

photograph themselves and/or their client when clocking into a shift. If the system fails to prove a match, then that worker log-in is flagged for further review, and can result in lost or delayed wages. Although it is not required by the mandate, EVV vendors such as FreedomCare and Direct Care Innovations use facial verification. In addition to privacy issues, the use of this technology raises concerns over workplace bias and discrimination. Facial recognition technologies have well-documented racial and gender biases, showing lower accuracy rates for identifying people of color, particularly Black women. These biases apply particularly to the U.S. homecare workforce: nearly 90% are women, 63% of whom are women of color.[5] Facial recognition technologies also raise concerns over consent and coercion, as older adults and people with disabilities may be pressured to choose between opting into biometric data collection or losing access to critical services. Workers may similarly feel pressured to coerce their clients into complying with daily biometric data collection in order to do their jobs.

- **Voice Verification**: Some EVV systems also use voice authentication, a form of biometric surveillance which requires a worker and/or their client to speak into their phone in order to match their voice to an existing voice record. Interactive Voice Response (IVR), often referred to as "voice verification," requires the Personal Care Services (PCS) worker and/or consumer to login and out using biometric voice authentication on a landline or cellular device, raising privacy concerns associated with collecting, storing, and using such biometric information. Service recipients have also expressed that their autonomy can be limited by IVR in situations where they experience speech disorders, which can prevent IVR from properly recognizing their voices, thus resulting in non-compliance with EVV.[6]
- **GPS Tracking and Geofencing**: The EVV mandate requires that workers must log the location where services are provided when clocking in and out. In EVV systems, this is achieved through the GPS location tracking capabilities of the worker's smartphone. Geofencing is the practice of setting geographic perimeters around a location, and is used to limit where workers are allowed to log their work. Because home- and community-based services are integrated into service recipients' everyday lives, digitally tracking workers' location data also generates extensive digital maps of service recipients' movements, as well as that of their families and

[5] Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," Proceedings of Machine Learning Research, 81 (2018): 1–15.; http://phinational.org/resource/direct-care-workers-in-the-united-states-key-facts-2/

[6] https://healthworkforce.ucsf.edu/publication/impact-electronic-visit-verification-evv-personal-care-services-workers-and-consumers

> social networks. Service recipients also expressed fears that their location data could be scrutinized and misconstrued to justify denial of services. In some states, geofencing has been used to require that workers log their work only within approved service locations, which entrenches ableist assumptions that service recipients are homebound. For many service recipients, this form of surveillance enforces a state of de facto house arrest by limiting their movements. To date, regulators have taken little action to limit either feature, despite both features pressurring service recipients and their workers to re-orient their lives to conform with compliance rules and avoid being flagged for potential fraud.

EVV's place at the center of labor, digital and care concerns

Pressures to follow EVV system rules often strained employment relationships, as workers struggled to make their work visible to digital systems. In some states, exasperated service recipients described placing reminders all over their homes or setting up dozens of phone alarms to keep up with constant electronic check-ins. Even small errors in compliance could lead to delayed or lost wages, and any deviation could result in a convoluted negotiation with healthcare bureaucracies. Poor system design and a lack of transparency made workers wary of invasive data collection, while geofencing requirements significantly limited service recipients' abilities to move freely in their own communities.

In addition to the immediate harms, the rollout of EVV systems and similar data-centric technologies that use biometric surveillance might have further-reaching impacts to U.S. care infrastructures. Some advocates have argued that the EVV mandate undermines many of the gains won by the disability rights and Independent Living movements in their push for the right to live independently in their communities rather than in institutions. Furthermore, growing surveillance and compliance burdens on service recipients may create barriers to accessing critical services in ways that are substantial but not easily measurable in the long-term. It's also possible that data generated by EVV systems could be used in the future in ways that data subjects have not consented to.

2. Governance and Stakeholder Engagement Recommendations *(Questions 6a, 6h)*

Through the process for developing a Bill of Rights for an Automated Society, we encourage OSTP to examine the consequences of uncritical adoption and government mandates for use of biometric technologies. The government has a responsibility to understand the full implications of adopting technical systems with such expansive and unexplored social impacts, particularly for communities that rely on government services and are increasingly having their interactions with government institutions mediated by biometric technologies.

In this effort, we emphasize the following recommendations:

1. OSTP should support federal agencies in their efforts to better understand the use of automated systems in public benefits delivery, and ultimately recommend the prohibition of technology that further marginalizes and harms the communities who are entitled to benefits and care.

The United States is experiencing a care crisis that has been exacerbated by the COVID-19 pandemic, including a shift away from institutional care settings as occupancy rates in nursing homes and other congregate-living settings dropped sharply across the country. Government efforts to invest in and reform the country's care infrastructure have been met with significant contestation over funding. Investment in these programs would include wage increases and better training and benefits for workers, as well as enhanced quality of care and expanded access to services to more people who need them.

Labor, disability, and elder rights advocates have warned that the current system is ill-equipped to meet growing demand. **Rather than heeding these calls by expanding services and investing directly in the workforce, government actors have often instead deployed new technologies to recalculate the distribution of already thin resources, or to police, surveil, and restrict those who receive them.**

These systems' inability to factor in the subtleties of individuals' care needs led to drastic service cuts with devastating effects to service recipients' health and well-being. These measures may serve the interests of controlling costs, but ultimately do not address the underlying state of chronic underinvestment. Furthermore, because this technology is designed in order to further institutional aims like cost-cutting, rather than being designed in response to the needs of care workers and recipients, it will likely continue to result in further harm and flattening of the complexity and interpersonal nature of care and support work.

The assumption that automated systems can be used to reduce fraud and increase efficiency is compounding inequality in the way that public benefits are delivered. These attempts to reduce fraud cannot be understood outside the context of racism, sexism, and the deep stigmatization of poverty and disability that have long shaped labor and care infrastructures in the U.S. Unlike fraud oversight practices that focus on institutional accountability—such as audits of home health agencies' billing practices—EVV systems direct the digital surveillance spotlight onto individual workers and their clients' daily lives by perpetuating an environment in which the default assumption is that everyone is committing fraud and cannot be trusted.

This is consistent with widespread digital surveillance of low-wage work, which is rooted in racist perceptions of the workforce as unskilled, untrustworthy, or lazy. Extensive surveillance—both subtle and overt—has long been normalized in the context of low-wage work. Rather than focusing on improving workplace conditions—including poor wages, lack of benefits and training, lack of access to technology, and overall social devaluation—policy efforts are instead marshalling technology to more closely monitor and discipline the workforce.

The failures of EVV go beyond poor user design and failed implementation and extend to serious questions about whether this technology improves job or care quality. Our research indicates it does not when its users' needs are not prioritized. While data-centric technologies are often hailed as solutions to social problems, EVV demonstrates how the government's use of data-centric and biometric technologies is often guided by punitive aims that reinforce racism, sexism, and classism.

OSTP's efforts to highlight this dynamic could educate and inform other federal agencies grappling with these challenges, and could facilitate a more holistic reckoning with the government's use of data-centric and biometric technologies.

OSTP could also take steps toward recommending the prohibition of the use of such technologies in certain contexts absent effective oversight. Leaving this set of governance concerns up to companies through self-regulation, company principles, and other "responsible AI" initiatives is not going to result in meaningful checks on harms, particularly to historically marginalized groups who are already radically under-represented in the design of predictive systems.

2. OSTP should commit to research and policy proposals that center community- and justice-informed uses of algorithmic systems.

We need to question both the centrality of tech companies in relation to the state provision of services and benefits, and the ability of the companies' technologies to serve vulnerable communities in ways that don't further unjustly criminalize them. **Instead of calling for the elimination of all technology in care and labor contexts, our research indicates the need for greater visibility of the harms technologies can create, and a deeper commitment to community-oriented policy approaches that ensure any technology deployed in the provision of public benefits and services is subject to more meaningful democratic deliberation.**

In the years following the 2016 legislation mandating EVV, public backlash emerged as service recipients and workers struggled to adapt to the new requirement. Dozens of town halls across the country surfaced deep confusion among EVV users over opaque policies and glitchy, inaccessible systems. In a 2018 stakeholder call hosted by the Centers for Medicare and Medicaid Services, officials summarized the public input they had received from around the country: this included significant concerns over privacy, financial and administrative burdens, and fears that EVV would exacerbate labor shortages and push service recipients into institutions or out of Medicaid entirely.

Public input and participation in an accountability process is not synonymous with accountability to the public. The timing and nature of the public engagement, who represents "the public," and the response to that input by the institution controlling the technology all matter deeply.

These issues are emerging at a time when tech companies are looking to enhance the scope and predictive power of their products. Despite significant implementation failures involving more rudimentary technologies, multiple state governments have already adopted powerful, automated-decision making tools to assess disabled people's eligibility for Medicaid and home- and community-based services, often with little public debate or transparency over how decisions are made. While it is unclear whether EVV-generated data has yet been used to cut services, it is one potential trajectory for future use of the technology.

Moving forward, we encourage OSTP to support federal and state governments to think expansively and creatively about stakeholder engagement, drawing on communities' lived experiences of algorithmic systems to determine whether and in which ways existing regulatory tools can be applied to mitigate algorithmic-driven harms. In instances where those tools are not sufficient, we encourage close collaboration with labor and disability rights coalitions to imagine and implement alternatives that are responsive to community needs.

Resources and Further Reading

Our research outlines many instances in which labor and disability rights advocates foresaw the harms that EVV systems would bring. Many groups have continued to advocate for alternative policies, including a ban on the use of geolocation (GPS) and biometrics by EVV systems. The following resources significantly informed our work and provide additional analysis on the impact biometric technology is having on care workers and care recipients.

- The National Council on Independent Living, Electronic Visit Verification (EVV) Task Force Statement of Principles and Goals
- Kendra Scalia, Electronic Visit Verification (EVV) Is Here: What you need to know and how to get involved
- Stop EVV, Electronic Visit Verification (EVV): What It Is and What It Does to Our People
- Alicia Hopkins, How Electronic Visit Verification Is Harming People With Disabilities

Sincerely,

Alexandra Mateescu, Researcher
Serena Oduro, Policy Research Analyst
Brittany Smith, Policy Director