Sharon Seidl
177 Ashford Ave
Dobbs Ferry, NY 10522
Phone: 623-760-5410
Email: sharon@goodonit.com
Sharon.seidl@consumer.org

Thank you for giving me an opportunity to speak with you today. I am hoping my story can be an example of how dangerous it is to not have effective rules to protect consumers from unregulated privacy practices.

A little about me…
I work in the field of technology and I have researched technology my whole life. I recently worked on all of the displays for the Orlando Science Centers Artificial Intelligence Museum which opened this last September and so I have a background in understanding machine learning.

Beyond my work passions, I am also single Mom of 3 adopted foster children. My 3rd child Bella has suffered 3 skull fracturs and 2 broken arms by her biological parents. When they did this to her – they did not know that she also had a very rare disease called Tuberous Sclerosis Complex.

With TSC your missing chromosomes that fight non-cancerous tumors from forming. So she has tumors on all of her vital organs. She has over 200 doctors appointments per year, as well as, epilepsy and cognitive issue. I depend on state funded home health aides to manage her disease and care while I am at work.

Recently, the agency I use, informed me that they intended to use an app for their workers to clock in and out of. I was curious and downloaded the app on my phone and read the privacy statement. I immediately became concerned with dangerous language in that document. Which stated that the app would be tracking my daughters' location and that it would allow for 3rd party access to all of my daughter's information.

So, I called the agency to ask them about it. It was then that I learned about Electronic Visit Verification and the Cures Act Law.

I then began to researching what other agencies were doing with EVV compliance. I found that many Electronic Visit Verification apps are collecting more than the federal law requested, like continuous location data, biometric data, and listening in. The apps also send push notifications and track when the notification is or isn't answered.

I also found out that the data collected included her Medicaid IDs, her Insurance IDs, her diagnosis codes, age, location social security and our addresses of the home. Many EVV apps have the ability to listen in and collect biometric data.

It is such a violation to not only my daughter's privacy and rights, but a violation on our entire family. And now along with managing this awful disease I am now forced policing my daughter's information which could be violated in the worst possible way.

I ask everyone in this room for one moment think about what would it feel like if you needed to **verify your identity and physical location** with your state government via a **GPS-enabled biometric device** every time you exercised a civil right? Like going to a doctor? Or having a medical emergency or needing to go to the pharmacy and buy private personal items. And if your helper didn't properly check in, you ran the risk of losing that right — or of losing your health? And that this is happening to your child who has no ability to fight for their own rights.

What would it feel like if the government then outsourced the responsibility for managing that check-in process to a **third-party contractor** that who's only motivation is to make money on a law – with no regard to HIPPA or PRIVACY.

And if you didn't comply you would lose all services and possibly die. Or worse your child would die.

SO, I did what any feisty citizen would do and began to research the law and reached out to Medicaid at both the federal and state level. You can see those emails attached.

I also researched everything I could find out there on Electronic Visit Verification - who was leading this – were there other citizens as outraged as I was. I did find many stop EVV groups and organized change.org petitions as well as Facebook groups. Thousands of citizens outraged by their concern for privacy. It is frustrating because no one can answer my privacy concerns on either the state or federal level. My feeling is that no one on these levels knows enough about data and how it is accumulated – so they do not know enough to be concerned.

The big problem is that it's the tech companies who are building these apps, are bending the law so that they can charge this back to the states and agencies an overly excessive expensive solution where the tech companies manage the data and control what is collected.

These companies are scarying the states and the Fiscal Intermediaries into services that the EVV law does not require.

Even worse is this idea that these tech companies **may not have secure servers or information security officers employed to protect this data in their offices** – meaning my daughters' data would be sitting just waiting for predators to take advantage of her information. Forcing millions sick and disabled individuals into policing their data from hackers on the dark web.

It is not a matter of, if this data will be breached, it is a matter of WHEN.

So far this year there has been over **50 million** individuals effected by health care data breaches. That number is climbing – you can see that report also attached. With such staggering numbers

It is mandatory that we enact some strict regulations with regards to personally identifiable information.

One of the largest costs to the Medicaid system is not the disabled community taking advantage of the system, it is going to be fraud from stolen medical identity. Where fraudsters use stolen data to create fake IDs – or to buy medical equipment and attain drugs that can be resold. Also they will be able to use that personal identifiable information to pose as an individual to get medical services under someone else's Medicaid identification.

The Federal EVV Law only requires these 6 items.

1) the type of service performed;
2) the individual (name) receiving the service;
3) the date of the service;
4) the location of service delivery;
5) the individual providing the service; and
6) the time the service begins and ends

The law **did not** say that it had to **PHYSICALLY LOCATE** my daughter through **geolocation**. Only that the location needs to be disclosed home or not home.

It **does not** say that they need to take a photo of my daughter **or use her biometrics and fingerprint** in any way. It **does not** say that they need to **attach her personally identifiable information**, like her social or her insurance id's or her diagnosis codes. It **does not** say that they have the right to send push notifications to the app forcing her workers to stop and answer. It **does not** say that the app has the right to go in and listen to the worker while they are with my daughter. And it **does not** say that my daughter needs to be a prisoner in her own home.

Allowing 3rd parties to collect data is a slippery slope. If you allow this to happen to the disabled community. Does this then start happening to all?

It's rare that data gets collected for just one purpose and that data is restricted to just that purpose. As I know from working in technology, often companies collect data for the purpose of monetizing it at a later date.

When caregivers log into a GPS-enabled EVV devices, they *also* provide a precise and analyzable location history of the clients, **and by implication a record of private and Constitutionally-protected behavior**.

This data gets **enhanced by machine learning techniques**: data is never just about the thing you originally think it is, it is always also about what can be mechanically inferred to be used later for another purpose.

I recently read a story from Karin Willison on the disability-rights blog *The Mighty*. She has cerebral palsy and requires PCA support to pursue her very active life (which includes a delightful wheelchair travel blog with plenty of service dogs). While vendor-produced instructional videos about EVV portray the process as simple, they do not highlight that automated "verification" always includes a check against a baseline.

How does the system know to trust a **geolocation** input? It checks that input against a baseline set of common locations or previous locations, such as one's home, school or church.

While using the app the client is teaching the system what those locations are, and **if service is rendered at an "excessive" distance from one of those locations, then the client will have to log on to a web portal or speak on the phone to explain the "exception event."**

Yet if a client like Karin is constantly out and about, much of her life will be an exception event. Disability advocates have warned that this type of data surveillance is effectively house arrest. In a computer system, trust is coded as acceptable variance from a norm, and how an EVV system surveils that variance says a lot about how we assume disabled people should live their lives.

The system warns the agency and forces the disabled individual to justify their activities. The disable individual must verify their whereabouts to a corporate call center and must teach the system of their behavior or she will lose her services and perhaps her independence.

In Senator Thomas's proposed legislation, from May of this year, he offered some critical points that should be considered and should be implemented across the board with privacy practices.

High up in this article was word - #2 the word was "CONSENT"

The line reads:

2. "consent" means a clear and affirmative act establishing a freely given, specific, informed and unambiguous indication of a consumer's agreement to the processing of personal data relating to the consumer, such as by a written statement or other clear affirmative action.

Through out this article the legislation suggests that consumers should have **the right to know** what the information is that is being collected and **HOW** that information would be stored and used.

(These will not be read at the hearing unless time permits)

Here are some ideas on a better way to handle the Electronic Visit Verification federal mandates:

1. The federal law does not require logging precise geolocation data, only "location." That may be satisfied through many different design choices, such as a simple binary radio button offering "Home/Not Home" as options. Demand design practices that collect minimally invasive data. And allow for consumers to Consent to that data.

2. "Exception events" triggered by EVV systems must be rare for all users. Default settings that impose additional reporting burdens on even a small number of clients and care providers create an unacceptable cost on the right to community-based care.

3. **No biometric or geolocation data, nor data that can be used to infer Constitutionally-protected activities**, should be collected unless it serves a specific, discrete purpose that cannot be accomplished otherwise and adds a clear value to the client and caregiver.

4. If geolocation data is recorded, it must be disposed of after a reasonable period for auditing, such as 180 days.

5. Even if geolocation data is logged in the EVV system only when a shift change is triggered, that still creates machine-readable patterns from which behaviors can be inferred. Additionally, the device itself may record GPS regularly in its RAM even if it is not reported. Without technical details this is challenging to determine, so manufacturers and service providers must provide those details and use open source software that allows verification of their claims.

6. Data collected via EVV devices, particularly geolocation and biometric varieties, must not be repurposed for use by commercial third-parties, including subsidiaries and commercial partners. A hold or NO SALE rule must be in place – especially since this data includes Medicaid IDs as well as personally identifiable information.

7. Data collected by EVV should not be available to law enforcement without warrants, and there should be no pipeline of EVV data to other governmental agencies without anonymization and aggregation.

8. Medicaid agencies and product manufacturers must explain in clear, concrete terms when and how EVV devices collect visual and audio data. If audio or visual data collection is

disabled (*disabled* is different from *not used*), explain whether that is done via software or hardware alterations, and explain whether those alterations could ever be reversed.

9. It is not appropriate for agencies to provide "alternative" reporting methods to deeply flawed default or preferred methods. The default or preferred method should be privacy-preserving and appropriately designed.

10. Device/app designers should adhere to NY State laws regarding privacy rights. These apps should be held to the same standards in that area.