Data Privacy Context & Analysis of Substitute HB 1155 (h-1001.1/23) Rep. Hansen

Maya Morales, founder
WA People's Privacy

This analysis, while undergoing multiple drafts, has not been reviewed by any other parties at the time of publishing due to time constraints. Please excuse any typos or small errors. This is people's (unpaid) advocacy! Not the product of a salaried team of lawyers and editors. I've made no attempt to adhere to a style guide or conventional bill analysis standard. This is just straightforward work product.

Important note re the Civil Rights & Judiciary Public Hearing and subsequent executive session this sub bill came out of: Chair Hansen did not permit WA People's Privacy, nor several other individual testifiers who all signed in PRO on the bill, to testify in this bill's public hearing, claiming insufficient time, in spite of several signing up far in advance and some even making a rare trek to Olympia to testify in person due to the deep importance of this bill. All tech and business industry lobbyists who signed up *were* permitted to testify (most signed up OTHER), and were openly invited by lawmakers to follow up afterward with their requested amendments and carveouts.

Introduction

GRATITUDE

Drafting and laboring over this document has been a big challenge, but it's also been a gift. I appreciate and offer appreciation to the drafters of My Health My Data (HB 1155/SB 5351), and the bill's main sponsors. This bill is the strongest data privacy bill that has been granted a hearing in the WA Legislature in recent years, and it is a huge honor and a gift to be - personally, and as an organizing entity – in the right place at the right time to able to read, support and analyze this bill alongside other advocates, and to be organizing for data privacy in these times. Thank you, Representative Slatter, Senator Dhingra, Attorney General Bob Ferguson and the talented and committed team in the AG's Office for bringing forward this bill.

THE INTENTION OF THIS BILL ANALYSIS

This analysis is meant to be helpful to people doing people's advocacy, *and* to our lawmakers who would like to advocate for data privacy post-Roe. Legislation can be dense and hard to understand. This document makes an effort to explain what each seemingly small change means, and the cumulative effect of changes when understood together. The need for this document arose when Chair Hansen's substitute bill was accepted and voted out of the House Civil Rights & Judiciary committee, because this is no longer the same bill. Some really important protections have been removed or dismantled, and because the bill covers all health data, the dismantling of those protections *would* impact *all* WA residents, *and* abortion and gender-affirming care seekers.

The following introduction to my analysis of the bill's changes summarizes some of the context from which our advocacy work on this bill emerges. Headings and a Table of Contents are

provided for people with time constraints. That being said, we'd like to encourage you to steal a moment outside of the time-constrained hyper-efficiency boxes we are all too often bounded within, round up some snacks, tea, coffee or a beer, and take a moment (or several) to read this *as story, and as herstory*, and to appreciate our relationship to this lawmaking process.

THE CONTEXT

The decision to house the drafting, conversations, and advocacy on this bill exclusively within the frameworks of a small group of reproductive rights & reproductive justice organizations unfortunately left out key voices and perspectives. HB 1155/SB 5351 is *a data privacy bill* concerning people's health data, and seeks to create law that regulates the collection and sharing of health data (not regulated by HIPAA) by companies who fall within the bill's definition of "regulated entities." It's actually really exciting, and really good for Washington residents, that a data privacy law includes all health data, but that's also why it's so important to have more stakeholders with non-industry perspectives on privacy in conversation with this bill.

Reproductive rights and justice organizations have been doing *vitally important work,* and have been laser-focused, *rightly-so*, on the long-term fight for the right to abortion healthcare, people's access to that care, educating people about our rights to abortion healthcare, and doing everything possible to remain one step ahead of the complex legal landscape of abortion case-law and legislation across the U.S.. It's *a lot, it has always been a lot,* and we have the utmost appreciation and respect for that work.

We've been deeply worried that the staff of some repro rights-focused organizations we've communicated with about this bill may not have the kind of experience reading data privacy laws that allows them to quickly flag the difference between a tricky bill definition that is protective, versus one that's been nuanced to create a bad loophole, specific to the way data is collected, stored, processed and moved (data flows) via many different platforms and devices. For instance: a definition of de-identified data and a de-identified data exemption that may at least provide a *few* guardrails versus one that actually green-lights the very risks and harms these organizations want to interrupt. Never mind the technical awareness that the blanket exemption of all de-identified health data in and of itself is a *huge* threat to abortion care seekers, and a growing threat to everyone else.

To us, this speaks to the vital importance of ensuring cross-movement involvement, ownership, organizing and advocacy when it comes to data privacy and tech justice work in the legislative space, *and* mainly, the importance of ensuring that data privacy bills are proactively workshopped with, and supported with organizing, lawmaker education, and messaging *by* local grassroots organizations and individuals who are actively and *specifically* doing data privacy and tech justice advocacy, preferably those who are not industry-involved, industry-supported and funded, or industry-dependent.

IN THESE REPRO STREETS: LAW ENFORCEMENT & SURVEILLANCE

Just after the Dobbs leak, on May 3, 2022, we addressed the urgency of securing people's data privacy with a large crowd of demonstrators. And in the weeks leading up to the SCOTUS decision, we cross-pollinated the issue with other local, state and national organizations.

After Roe's overturn, we collaborated with other organizers and organizations to call for strong data privacy laws with our lawmakers at all levels, *always* highlighting the increased risks and surveillance threats on privacy post-Roe.

Last summer, we joined a group of organizers and UW Center for Human Rights researchers to discuss the risks of Automated License Plate Readers (ALPRs) and their disparate impact on immigrants and abortion healthcare-seekers. At the same time, WA People's Privacy had plunged head-first into cross-state and federal advocacy, working hard to make sure that people in our state would not be preempted from passing strong consumer data privacy laws by preemptive federal legislation that did not protect people's location data. We also spoke up in the FTC's public rule-making process on commercial data surveillance. It was clear that we had to prioritize the fight to preserve WA's ability to pass strong data privacy protections if we wanted WA to be a state in which people could safely access gender-affirming and abortion healthcare, and a state in which people could work to secure all of our rights and liberties into the future – particularly looking toward the vast expansion of AI, virtual interfaces, and biometric-involved data collection, machine learning, and automated decision systems planned by large corporations and mega-investors and edging into our immediate horizon.

Also in May/June of 2022, we joined up with several Seattle area organizers to create some public education materials about six invasive surveillance technologies used by SPD, and helped to drive public comment on these to the City Council, *all while understanding and expressing that the overlap in policing surveillance tech and abortion care/gender-affirming care access for women of color and trans people is real.* We then followed up with a push for a

second round of public comments this month. The hearing to review proposed amendments to their use by City Council was held February 22nd, and the use of all six technologies was approved. These will be up for a final Council vote this week, with very little time for members of the public to parse through long and confusing documents, read and compare the amendments to the recommendations of the working group, collect their concerns and thoughts, and meaningfully engage their council members prior to a vote on Feb. 28th.

Last October, we joined Fight For the Future's calls to end abortion surveillance, and to corporations to require encryption for private messaging, and Make our DM's Safe. We then participated in a small meeting with Meta/Facebook to advocate for universal encryption of DMs across all of Meta's platforms.

Additionally, WA People's Privacy came together with Seattle organizers and community members last November to help stop ShotSpotter from being purchased and implemented by Seattle. ShotSpotter is a surveillance operation in which cameras and sensitive microphones are installed across neighborhoods under the guise of preventing gun violence by detecting gunshots. In fact, this tech doesn't prevent violence, and instead targets and surveils communities of color, with a network of live, recorded audio and video surveillance feed that can be shared with law enforcement and other companies. ***In this work, too, we recognized the intersection of reproductive and gender justice with law enforcement surveillance, and its disparate impact on women and trans people of color.***

We are doing this work because the undeniable truth is that securing safe access to abortion and gender-affirming care *is anti-surveillance work.*

The **enforcement of abortion and gender-affirming care bans is *in* the budgets** and **at the hands of law enforcement** agencies, local police, and even liberals who turn a blind eye to commercial data surveillance, and are apathetic to holding law enforcement accountable for a long history of terrorizing immigrants and communities of color, as well as radical-right & religious extremist individuals and groups – *all* of whom **support and prop up the policing and surveillance of our bodies as a solution for safety, which it *clearly* is *not*.**

WA People's Privacy *has consistently addressed the intersection of data privacy and abortion, because we are fighting for people's privacy. All of the time. Across movements.*

Privacy: not as an abstract idea or right, but as a real and necessary solution for us to preserve the ability of our communities to thrive.
Privacy: as the root that sustains our rights to our own minds, hearts, and bodies.
Privacy: as a safe pathway in the difficult terrain so many of us are trekking through toward racial, climate, reproductive, economic, housing, labor, gender and social justice.
Privacy: as necessary to keeping all of us safe and creating space for our joy and creativity.

It's critical to understand and actively hold awareness in all of our organizing (and law-making) that all of our fights for justice intersect. Privacy *is* central to *all* of them. Injustices do not exist in silos, and thus neither can their solutions.

WA DATA PRIVACY BILLS & MY HEALTH MY DATA

Late 2021, I joined up with many dedicated individuals and groups in what was then year *four* of efforts to ensure our state did not pass a consumer data privacy law that would basically "check a box" on privacy, while making current data practices and data flows perfectly legal, and leaving us unprotected *and* without legal recourse for who-knows-how-long into the future. I founded WA People's Privacy in early 2022, and it's grown from there! To our knowledge reproductive rights groups were not deeply or actively engaged in that data privacy advocacy.

Now, in WA's 2023 Leg session, we have a health data privacy bill in WA state that is being *primarily* workshopped with repro advocates who are deeply worried about a possible restrictive court ruling on medication abortions, while still desperately trying to protect people's access to that medication, and to clinics, funds for care, and providers' ability to offer that care post-Roe. We are one-hundred percent in solidarity *with* them in worrying about the women and trans people in our state and adjacent states who will need every shred of privacy possible in order to safely access care in the face of law enforcement surveillance via commercially available data. *Data that the substitute bill for My Health My Data will still allow access to.*

WA People's Privacy made three requests in our initial written testimony to the Civil Rights and Judiciary Committee to support and strengthen WA's original My Health My Data bill. Our first was: do not weaken this bill. Our second was: make sure the bill covers all health-data-collecting entities, including state agencies. The effect of the exemption of state agencies is that student health data, public health plan data, Dept. of Corrections health data, and any health data collected by city and county governments will not be afforded the same protections as the data collected by people who can afford to pay for private healthcare services and private health insurance. We immediately understood that when public entities utilize a third party or third party software – as they virtually all do, that data would not be extended *any* of these protections, because those public entities are not regulated entities under this bill, and thus their "processors" (previously "service providers") would also go unregulated. Not good.

We called out that this would create a non-standard application of health data privacy in WA state, which would privilege wealthier people who access health services *outside* of the WA Healthcare exchange and Apple Health, and disadvantage people who access all health care via government agency-mediated plans and services.

Our third request was to remove the "de-identified data" exemption. The effect of leaving in a weak definition and exemption for de-identified data is that this law will simply and legally green-light the very same predatory data-sharing and brokering practices that the law says it seeks to prevent.

In our view, if any further weakening changes or amendments were to be accepted, this could put My Health My Data at risk of being little better than the bad WA Privacy Act (WPA) in its application – a bill WA lawmakers and residents, including our Attorney General, rejected as being insufficient to protect WA residents, multiple years in a row.

The major difference between the climate surrounding MY Health My Data and the bad WPA of past years? Repro groups being positioned as the lead advocates on the bill.

With that comes the risk of My Health My Data being given the unconditional rubber stamp of approval by WA chapters of national reproductive rights organizations and "industry partners," no matter how many bad (further weakening) changes are made, and we are deeply worried about that.

We are concerned the CR&J's Substitute Bill could be passed under the guise of being "a very strong bill," when in fact, this substitute bill now contains many of the same weaknesses and loopholes that the Bad WA Privacy Act did, some new ones, and some of the same loopholes we opposed in the preemptive federal data privacy bill (ADPPA) last summer.

THE DETAILS - WHY THIS ANALYSIS COMES NOW

The current House Substitute bill for My Health My Data, which is on the cusp of the passing the house very soon – likely with unanimous Democrat support because it's being billed as a win for abortion healthcare, will continue to allow abortion and gender-affirming care seekers to be targeted via our "de-identified" data, location data, as well as geofences. With these new, altered, nuanced and/or weakening definitions and bill sections; the sub bill is set up to do some pretty messed up things. It will subsume some previously protected categories of "personal data" into being easily classified as publicly available information, and therefore not covered by the bill, and it will do significant damage to the public transparency provisions in the legally required privacy notices that companies must post on websites. These privacy notices would not be required to inform people of specific details, like the types of data they collect, for what purposes, and exactly with whom that data is shared, and for what purposes, and exactly who data is sold to, and for what purposes. Instead, companies can just generalize. This is really bad, and creates bad precedent for weak consumer law, ineffective privacy protections and poor transparency requirements that could actually erode the stronger protections in other states and federally over time. Since My Health My Data actually covers *all* health data, and *not* just reproductive and gender-affirming care health data*, these are not good precedents for WA to set generally, given they allow everyone and anyone to be targeted by these flaws for any health data.* The bill also creates a pay-for privacy framework, and serious consumer safety, transparency and accountability roadblocks via prohibitive, problematic and lengthy processes for requesting the deletion of data, 'authenticating" that request, refusal, appeals, demanding fees, and limiting people's requests to twice annually as if our health data was a credit score.

In our view, the substitute bill runs the risk of "pink-washing" - perhaps more accurately "repro-washing" – big tech's agenda, and allowing the industry to *finally* have their hand in sneakily passing a weak data privacy bill in WA state under the guise of protecting abortion healthcare. Not only a weak bill, really, but one that sustains the current harms to abortion and gender-affirming care-seekers, and all WA residents. All health care data is extremely sensitive. That is why it's vital to get into cross-movement coalition and fight for strong data privacy bills, ensuring that cross-movement eyes are on this bill, because it will have a huge impact all of us.

We're simply not OK with tiptoeing around these issues. *It is extremely important to speak and name the actual problems this bill needs to be designed to confront, with utter clarity, while there is till time to offer remedy.* The good news, we DO still have time to find remedy.

Let's be reminded that although this *is* a consumer law, the need for this consumer law arises out of the real risks and harms to people accessing essential care that has been declared *not a personal right by our highest court, and thus made illegal to access in states across our nation, including our neighboring state of Idaho.*

Said another way: lawmakers' awareness of the need for this law arises <u>because</u> police and law enforcement access to commercial data presents a clear and present danger to all women and all people seeking abortions and gender-affirming care. One of the main goals of this law is thus to stave off violence, harm and arrest of people who are simply trying to access care and exercise our bodily autonomy. But because this law applies to all health data, it will greatly benefit many more people if it is passed in the strongest possible form, preventing many other types of health data harms.

It is in this spirit, and with the understanding of everything we have articulated about the broader and intersectional fight for data privacy, that we offer the following bill analysis of the Substitute bill for HB 1155, passed out of the Civil Rights & Judiciary Committee on January 24, 2023.

Our conclusion is that the cumulative effect of what some have characterized as "a few small changes, additions and minor amendments we can live with" in fact enact the kind of red-tape, difficulty, obfuscation, frustration and reinforcement of healthcare traumas that disproportionately affect poor and adversely impacted individuals and communities, and serve to reinforce economic, racial, and tech injustices.

We entreat our lawmakers to fix this bill by restoring its original strong protections in order to ensure that its intended consequences actually do come to bear for companies in ways that meaningfully protect WA residents: a basic opt-in consent requirement for the collection, sharing and selling of <u>all</u> consumer health data by any private entity so that people (consumers) are simply and easily able to protect ourselves from the intrusion of law enforcement and other interested parties into our personal healthcare matters, and are not obligated or coerced by companies to consent to any sharing or any selling of our health data in order to use a health service or obtain health care.

Substitute Bill - Analysis of Changes

This numbered list corresponds to the bulleted list of changes at the top of the <u>subsitute bill</u>, in the same order.

1. DEFINITIONS:
Adds definitions of "authenticate," "precise location information," "processor," and "publicly available information," and modifies definitions of "biometric data," "consumer health data," "geofence," "person," and "regulated entity."

[NEARLY ALL OF THESE ADDITIONS & TWEAKS WEAKEN OR NULLIFY THE PROTECTIONS IN THE ORIGINAL BILL.

NOTE: Some of these additions are *not* exactly new, rather changes to wording on existing terms definitions in such a way that they create new carveouts, loopholes and exemptions for current and/or future abusive data industry practices.]

We'll break these down one-by-one:

A. Adds the definition of "authenticate"

This definition (along with the new section requiring that people authenticate their identity in order to review and delete data) might just seem commonsense, right? Of course you should authenticate someone who's trying to delete their data!
Oops! Not so simple.

In reality, this puts into place something a lot more complex: a process that can actually strip people of the personal privacy protections they have already implemented, and that can place additional barriers to requesting the deletion of our data, or even prevent our ability to do so at all.

Companies can make this authentication process as sloggy, difficult or tricky as they see useful to their profitability. Way beyond just being annoying, this translates to harm.
People impacted by systemic violence and injustice, who are already suffering data harms amid many other harms, are much more likely to simply give up when these kinds of processes are burdensome, difficult to navigate and time-consuming. For anyone without access to a computer, these processes are often much more time-consuming on an inexpensive or older smartphone. For those who have very low tech-literacy and/or irregular access to any tech at all, an authentication process may even be unnavigable. For people who lack IDs, have lost them, or have abusive situations in which they have restricted access to their own ID, information and/or a device, this is definitive road-block.

So, this change will inevitably have disparate impact on poor and already-systemically marginalized and impacted people and groups, as well as elders and disabled people.

Authentication can be very problematic in terms of using apps, websites and data-collecting devices. For over two decades we've been struggling with a legal environment in which data privacy has been framed simultaneously as an individual responsibility and burden, *and* as the state's duty to violate in the name of war and law enforcement surveillance. Both of these are fallacies, but they *are* challenges nonetheless. So, people have taken their own, sometimes scrappy, measures to protect our privacy. OK, like what, you ask?

Well, due to concerns about the completely unregulated data flows of both private and public entities, as well as lax and fairly unregulated data security practices, many people attempt to protect our privacy by intentionally providing incomplete or inaccurate personally identifying information upon signing up to use apps, online platforms and devices.

So, if an "authentication in order to delete" provision is passed in this bill, it will likely require the verification of someone's *legal ID* in order to delete their data, because the authentication process has been left up to companies to determine. But, this can be super-harmful. Why?

1) it may defeat the personal protection of a user choosing to provide inaccurate or incomplete data when setting up a health app or service in order to secure their privacy,
2) it is very likely to lead to many deletion requests being denied when the legal ID an app or service forces user to to provide is not a match with the information user initially provided, and *critically:*
3) it backs us into normalizing the collection of *more* personally identifying information as a requirement to use *any* service or app, effectively laying the groundwork for normalizing the use of digital IDs as users and companies negotiate troublesome authentication processes that could inevitably lead to many refusals to delete, errors and user-appeals. Digital IDs have long been met with grave concerns by human rights defenders the world over.

In the context of post-Roe safety and security, hopefully people can understand that giving way to a sure shortcut leading to the rollout of digital IDs in a health data privacy bill – when we have *so* much farther to go in order to secure even our most basic rights to bodily autonomy, and our most basic of data privacy rights, let alone to develop secure methods of digital identification (which realistically may not even be possible), is a very unfavorable shortcut to unintentionally back ourselves into.

While providing inaccurate information is unlikely to stop wealthy, very technologically skilled, and/or state actors from invading privacy when they purchase bulk data (because all data must still contains markers that make the data useful and able to be sorted, filed, stored, shared and re-sold – and thus profitable, even *after* a person's name, address, age, race, and gender have been stripped from that data), it *is* still far less likely that an abusive partner, family member, or random stranger will be able to find and access their accounts.

Strictly speaking, this kind of scrappy individual privacy protection that people utilize – in the absence of strong data privacy laws with opt-in consent models – it's really more of a hurdle than a roadblock to violating a person's privacy, *but that doesn't mean we should get rid of it lightly.*

On the contrary, we should protect the right of people to secure our anonymity for safety reasons. We saw this battle play out in the past with Facebook (Meta) over requiring ID verification and the use of people's legal names. It harmed trans and queer people, trampled people's rights, and enabled stalkers.
So, we recommend getting more specific about how authentication may be done.

B. Adds (Modifies) "location" to "precise location" information

INSERTS the word "precise" in front of the current definition of "location" and thus changes the scope of protections in the bill, essentially removing the ability of people (consumers) to protect our location data at all, let alone protect it from bad actors.
And by bad actors, yes, we DO mean law enforcement agencies who will hunt down abortion and gender-affirming care seekers.

(NOTE: that the insertion of "precise" modifying location also necessarily shows up in other definitions now, modifying the definition of geofence and Section 10, as well as in the definition for "Reproductive or sexual health information")
We saw this same problem in the ADPPA (American Data Privacy Protection Act). Investigative journalists have looked into the ways that businesses, data brokers, and law enforcement obtain location data in order to hunt people down, and the facts are quite clear: limiting location data to a 1700-2000 foot radius does not protect people from being stalked and located, whether you call it precise or not. We're talking about the distinction of a location radius of about 4-5 city blocks. In suburban and rural areas that's basically precise, but it's still bad in a dense urban area when combined with many other sources of data about a person.

Our location data is accessed live and/or across time via many different methods, and police departments and law enforcement agencies are accessing our location more and more. Due to inter-local agreements and fusion centers, this data is often *easily* accessible to local law enforcement whether officially or informally. We need only to look to SPD's use of the "Geo Time" surveillance software currently under review by Seattle City Council to confirm this, but it's been a growing problem for years. See this 2020 Article from The Byte, "Cops are buying your social media location data without a warrant," where the author notes some of the shady practices of Babel Street, which recently required Rosette, or this 2021 article about the location data industry by investigative journalist Jon Keegan at The Markup.

People can absolutely be tracked to a clinic, pharmacy, or other health provider via the purchase of commercially available location data, much of it obtained in aggregate, "de-identified" form via data brokers like Lexis Nexus or even app developers, and easily re-identified with the use of its digital markers. Another big pool of location data is obtained by scraping the web for publicly available information. With the de-identified data exemption (and the removal of the prohibition on the sale of health data) it is possible to connect our location dots with great ease, and to thus conduct arrest, violence, or other harmful and nefarious activities toward people because of, or in connection with, our health data.

C. Adds "processor" (orig. bill used "service provider")

[ALSO, YIKES. BAD LOOPHOLES ALERT?]
This actually does appear to be a simple name change, and aligns the bill with the GDPR, which is fine. **BUT, this term is NOT included in regulated entities, and that kinda seems like a nuanced definition problem. Does that create a loophole?**

We also have questions about processors as it relates to distinguishing between WA processors and out-of-state processors, given law enforcement's easy access to an out-of-state processors' data. Since the key impetus for bringing this bill is to prevent law enforcement surveillance, harms, threats and arrests of people seeking abortion and gender-affirming care via commercially available data; it seems pretty important to address that somehow, even if it's a rather new and creative solution; but the sub bill doesn't seem to. I'd be happy to be corrected if wrong here, but the definitions of a "WA business" and "doing business in WA" do not seem to include businesses that are located and based out of state, and providing services to health providers that *are* considered WA businesses. Thus, we'd have: an out-of-state regulated entity loophole, in addition to the processor loophole generally, in addition the broad

exemption for all WA Health exchange service providers and contracts, in addition to now exempting entities that actually collect, sell and share consumer health data. Um...What?

Since "processor" is not explicitly listed as being a covered "regulated entity" in that definition, and since an entity that "collects, shares, or sells consumer health data" has also been completely removed from the definition of "regulated entity" in the bill, it would seem we now have a *triple, or maybe this is a quadruple,* loophole*?*

1) Companies that are "processors" aren't regulated 2) companies that "collect, share or sell consumer health data" aren't regulated (only those who *make decisions about how data will be dealt* with are covered - like, what even *is* that, y'all?) **3) out-of-state companies aren't regulated, and 4) the main companies that collect, share and sell consumer health data through WA Health Benefits Exchange via contracts** (like with processors, software companies and apps) **also *aren't regulated.***

But, I'm digressing into intersecting loopholes. Back to "processor."
Even if certain healthcare procedures are protected in WA, we do not have assurance that the data regarding those procedures will not endanger WA residents who leave WA and travel to a state in which their procedure or care is criminalized and their data is available. There are questions as to whether even the ability to access a person's *past* health records may jeopardize people's current safety given the ease with which law enforcement agencies can profile individuals via commercial data surveillance with basically no guardrails.

People move, have multiple state residences, or may even be transient across state lines. It seems like a good idea not to assume that we can have an overly simplified definition of 'protecting Washingtonians.' Shouldn't we be addressing how this law should apply to in-state *and* out-of-state processors, given the severity of abortion/gender-affirming care threats, and the complex surveillance harms via commercially available data across state lines?

D. Adds "publicly available information"

[LOOPHOLE ALERT - ALSO ADDRESSED IN STORY BELOW IN (D) IS "PRECISE LOCATION" VS LOCATION]
The addition of this definition is clearly with the express intention of creating loopholes for certain kinds of personal, health, and biometric data to be able to be exempted from protection and become fair game for data brokers and data prospectors, who have huge profit incentives to ensure they maximize the amount of data they have unfettered access to and can sell to law enforcement, research firms, think tanks, governments, and other corporations.

Given the way the definition of "Personal Information" now functions in relationship with this new definition of "publicly available information," – which was previously considered unnecessary and irrelevant to this bill – this is a loophole that appears nearly custom-made for companies exactly like Babel Street, securing a failsafe carveout that ensures that all kinds of health information that is collected with a persons' knowledge, can be automatically considered "publicly available information" and not protected under this law.

What constitutes 'with a person's knowledge' is a verrrrry squishy space. Businesses could get away with all kinds of deceptive and squirrelly practices in order to collect people's personal information if they can do without express affirmative opt-in consent.

For instance, if a person posts a personal, health-related story or incident on their social media page or on a health fundraising site, this bill allows all of that to legally be considered publicly available information, which can be sold, shared, stored, and utilized without any need to respect a person's privacy or ask for any consent.

Another example would be the collection of biometric information. If the legal obligation of "with a person's knowledge" could be satisfied as easily as posting a small sign, notice, or pop-up window with a message like, "Hey! We're collecting faces to bring you even better customer rewards when you shop here!" a *scan* of your face can then become public information. This is a really simple and easy example, but the kinds of biometric and other data that *could* be fudged into that category of "publicly available information" via methods that allow businesses to easily and legally claim that a consumer had knowledge, and thus their express consent was not required, and their personal information was fair game... it's not good, people.
And, over the next few years. increasing interactions with self-checkouts, wearables, robots, smart-home & commercial tech, and tech in public places that employ cameras, microphones and other kinds of sensors and tools; well, this just becomes an ever-widening loophole.

In terms of how this could affect abortion and gender-affirming care seekers right now, I'll try to unfold a data surveillance X abortion healthcare scenario in story form:

Let's say you're an Idaho resident seeking abortion care in WA, and several people know you're pregnant. Two of those people are your best friends, one is your partner, and one unfortunately happens to be your creepy anti-abortion, super-racist neighbor who is entirely too much in your business, overheard a heated conflict between you and your significant other about it in your yard the week prior (why did he have to yell it out like that? Argh.), and watches as you hurriedly toss your backpack into your car and drive off, not at your routine work-scheduled time, on a Wednesday - very unlike you. You had web-searched the clinic, called and made an appointment, googled and saved the directions to the clinic on your phone, and called in sick to work. Once across the Idaho border and in WA, you stop by a Wal-Mart to grab water, snacks and a pair of loose fitting sweats. While shopping, and again at the register, your face is scanned via face recognition-enabled software integrated with their store surveillance system (probably Clearview AI). ***You don't realize, but you completely missed the small sign posted near the doors that explained "Smile, you're on camera! We scan your face to keep our store safe!" Without you realizing it, this sign automatically made your face scan "publicly available information."*** So, your face has already been fed into a data stream used by Babel Street or other similar law-enforcement agency contracted service's data flow. Your exact location is able to be pinged, and able to be verified as soon as your face is matched with your financial data, based on what you purchased there on your debit card. Law enforcement got a warrant as soon as your neighbor called, and began hunting down all the info they needed to arrest you. When you're back home after your procedure, officers arrive at your home to arrest you (your neighbor leering at you through the window). You later discover police were able to track you heading toward the clinic after you left the Wal-mart using access to automatic

license plate reader (ALPR) data through an info-sharing agreement with law enforcement, and confirmed that you had visited the clinic via a socials post you made saying "I made it!" with a close-up picture of just your thumbs-up against your hospital gown, which you thought was maaaybe not the best idea? But it didn't show a sign or a building or anything, and you didn't realize it actually gave away your location, because you heard WA had a bill that protected that. But it was the *only* clinic within 2000 feet of that location, and WA's bill only protects your exact position *inside* that 2000ft radius, not your general location. *(obviously that's just the beginning of this horror story, but we'll end it here)*

Again, creating this loophole for personal information-easily-becoming-publicly-available-information via "having knowledge of its collection" without any need for express affirmative opt-in consent goes against the stated purpose of this bill. It sets up a current and future loophole rife with threats and harms.

E. modifies definitions of "biometric data"

[LOOPHOLE ALERT]
"removed and sleep, health, or exercise data that contain identifying information"
biometric data is definition (3)(b) in HB 1155, now definition (4)(b) in Sub HB 1155.

This change has been really concerning to data privacy advocates looking at the intersection of wearable devices, "smart" med-tech devices (medical technologies that use sensors and communicate and interface with systems that may involve automated decisions or feed into other complex algorithms), sleep-tracking mattresses and monitoring devices and their corresponding apps.

So, it may surprise some folks to learn that it's actually really important that sleep, health and exercise data *are* included in the definition of biometric data.

Even though "*consumer* health data" is elsewhere defined in this bill, we don't see that as being repetitive with or even conflatable with "health data" in the context of *this* definition. Here, we understand "health" as a more generalized adjective for medical and chemical states or signals being measured into data output - for instance, a measurement of the PH of your stomach by a digital pill that can track and create an alert about whether a person has taken their medication; or a brain wave monitoring device attempting to pinpoint certain activity in the brain; a tracking/monitoring bracelet for loved ones with Alzheimer's, alcohol monitoring bracelet, or a smart ring that measures heart rate, temperature, sleep cycles and activity; an glucose monitoring device that keeps track of blood sugar levels and syncs an app on your phone; a high tech contact lens that detects illness, or measures eye movements and iris dilation. All of this health data is sensitive and needs to be protected.

On the super-scary data harms side, wearable and/or home devices that collect biometric information such as sleep, health or exercise data can result in a data collector (broker)being able to build extremely granular and privacy-invading profiles on people to then sell. On the menacing side, future med-tech collecting and sharing/selling health data which is extremely specific to a particular illness or condition could lead to very serious harms in the future.

F. modifies definition of "consumer health data"

This change to "consumer health data" inserts the word "precise" in front of location, and removes a fairly broad sentence clause from the first sentence. It doesn't seem to have adverse impact on protections. Only the "precise location" problem, which is addressed above in (B) is objectionable. With "precise" taken back out, we'd be very happy with this definition.

G. modifies definition of "geofence"

This changed the definition of "geofence" by adding this sentence: "For purposes of this definition, "geofence" means a virtual boundary that is 2,000 feet or less from the perimeter of the physical location."

We go into this change and the larger re-wording change of the geofencing prohibition of 1155's section 10 later in this document (item 12). It basically creates confusion. This was modified to accommodate for the bill's weakening of location data to precise location data, but now it's unclear and *super*-awkward. The original definition was good, and the we should revert to that definition alongside restoring the original bill definition of location.

H. modifies definition of "person"

No commentary necessary here. This brings the law into alignment and harmony with a legal definition. It's just important for everyday folks to understand that when you see "person" in the bill, it's likely to actually refer to a company, whereas a single actual human being in the bill is called a "consumer."

I. modifies definition of "regulated entity"

[CREATES BAD LOOPHOLE]

This is addressed in "processor" amendment above as well: it seems that since data collectors, sharers, and sellers, and processors have all been completely nuanced out of being covered entities at all, this bill doesn't even regulate companies. The Sub bill definition also confirms in the "does not mean" clause that people with public health care plans will not be afforded the same rights and protections for their health data which is processed by service providers or contractors on behalf of government agencies. The very least WA can do, is cover *all* non-governmental health data collectors as regulated entities, even if there is an insistence on leaving government agencies *themselves* out of a health data privacy bill.

Please see the comparison chart and the note at the base of it provided below:

WA People's Privacy - Definition of Regulated Entity - HB 1155 Substitute Bill

Original Bill	Substitute bill
"Regulated entity" means any legal entity that (a) conducts business in Washington, or produces or provides products or services that are targeted to consumers in Washington; (b) collects, shares, or sells consumer health data; and (c) determines the purpose and means of the processing of consumer health data. "Regulated entity" does not mean government agencies or tribal nations.	"Regulated entity" means any legal entity that: (a) Conducts business in Washington, or produces or provides products or services that are targeted to consumers in Washington; and (b) alone or jointly with others, determines the purpose and means of collecting, processing, sharing, or selling of consumer health data. "Regulated entity" does not mean government agencies, tribal nations, or contracted service providers when processing consumer health data on behalf of the government agency
DOES SUB THE BILL CREATE MASSIVE LOOPHOLE BY REMOVING ACTUAL DATA COLLECTORS (!) FROM BEING COVERED ENTITIES, NUANCING THE WORDING TO COVER ONLY THOSE WHO DETERMINE THE *PURPOSE AND MEANS* OF COLLECTING DATA. BUT NOT THE ACTUAL DATA COLLECTORS, SHARERS & SELLERS (!!!)?? (NOR – AS WOULD MAKE SENSE PER THIS BILL'S DEFINITIONS – COVERING "PROCESSORS?"	

We're not going to mince words: this particular carveout (standing on its own) creates shameful inequity in rights and protections. But when combined with all the other tweaks... basically no one's really protected, so... (shrug)? It's all pretty bad.

2. Modifies the privacy policy requirements and provides that a regulated entity's privacy policy with respect to consumer health data must disclose:

- categories, rather than the specific types, of consumer health data collected;
- categories of sources from which the data is collected;
- categories of data, rather than specific data, that is shared; and
- a list of the *categories* of third parties and specific affiliates with whom the data is shared.

[WEAKENS ACCOUNTABILITY & THREATENS SAFETY - HIDES BIG DATA HARMS]
It's pretty easy for people unaccustomed to reading privacy law and policy to see this, and think OK, cool, yeah, totally fine. But it actually weakens the bill significantly from its original wording because HB 1155 doesn't define what it means by categories. Worse, it also creates a rule that is weaker that the standard for privacy policies under The California Privacy Rights Act (CPRA), for which compliance deadlines just went into effect on Jan 1, 2023.

We strongly recommend bringing SHB 1155's guidelines for privacy policy requirements WA My Health My Data into alignment or even a bit stronger than with CA's CCPA/CPRA guidelines about these disclosures. This will assist commercial entities in streamlining their compliance efforts on health data. In addition, it would be a strong solidarity move with CA.

There are concerted efforts to pass weaker consumer data privacy laws in multiple states in order to justify passing a preemptive federal law that will green-light many or most of the data industry's shady practices and preempt CA's strong protections. CA has been leading the nation on Privacy, so WA should catch up!

Under the CCPA/CPRA, people have the right to limit what "sensitive data" companies collect, how it is used, and whether/how it is shared. WA can bring our health data privacy law into alignment or beyond by adopting clear guidelines that define what is meant by "categories"(or

"types" if the AGO chooses to revert to types) in requiring that companies detail the categories of data that are collected, the *specific* data that fall within those categories, keep an updated and full list of the sources of data that is collected, and list all parties with which a person (consumer's) data is shared. Because of the way this change has been worded to exclude "specific data," and "specific types" and generalize sharing disclosures to "categories of third parties" rather than an actual list of third parties, it allows companies to be misleading and opaque.

For folks who may be not super-well-versed in this stuff, here's a more pedestrian breakdown of what this amendment would do:

WA People's Privacy - comparison chart regarding effects of privacy policy amendments HB 1155

Loose examples here, but hopefully these help illustrate the impact in the difference between Substitute and original bill in terms of the amount of info and transparency a company should be required to provide a consumer.		
Subsitite Bill		Orginial bill
We collect a user's "exercise data."	vs	Utilizing your wearable device and any other required or optional connected devices, such as your phone and wifi network, we collect the following user exercise data about you: Your speed, distance, gait/movement, pulse/heart rate, and other vibrations or fluctuations in movement and sound your devices' sensors collect which may provide information about periods of rest, in/activity, arousal, or sleep.
We collect data from your device.	vs	We collect data from your device, including through our app on your device; information about the other apps on your device; which services you access via our and other apps; your browsing history, IP address, advertising and persistent identifiers, location data (via GPS, wifi, and cellular networks), phone services utilization, and personal information - including name, address, phone number, email, health and personal background information you input into the device or app; your health information from any health apps you allow our app to access on your devices.
We collect data about you from other sources to improve our service.	vs	We collect data about you from other sources including credit reporting agencies, public records databases, and voter records; data brokers and data industry service providers, and other businesses and services you use or subscribe to.
We share information about you that helps us streamline our app.	vs	Information we share about you in connection with your wearable device: We share your data in aggregate form with other user's data with our affiliates, partners and subsidiaries, including: • your device information, your exercise data: your speed, distance, gait/movement, pulse/heart rate, and other vibrations or fluctuations in movement and sound your devices' sensors collect which may provide information about periods of rest, in/activity, arousal, or sleep.. • information about the other apps on your device, which services you access via our and other apps, your browsing history, IP address advertising and persistent identifiers, location data (via GPS, wifi, and cellular networks), phone services utilization, and personal information - including your name, address, phone number, email, any specific health and personal background information you input into your health history in the app, as well as your health information from any health apps you allow our app to access on your device. • information we have collected about you from our affiliates, partners, subsidiaries; as well as purchased from data brokers and service providers.
Who we share you data with:	vs	We share your data with affiliates, partners, and subsidiaries (list here) for the following purposes: (list here) We sell your data to the following data brokers and service providers (list here) for the following purposes: (list here)

Do you see the difference there?
This change would allow a regulated entity to have much more vague and obfuscating language in their posted privacy policy, and allow them to completely omit specific types and examples of data they collect, and from which specific sources they collect it.

The effect of this would be to make the data collection practices of companies completely opaque unless a person (consumer) utilizes one of their two allowed free requests to review their data. That would be a huge setback to the strides privacy advocates have made thus far, and it's pretty horrifying on a consumer level. How can you make an informed decision about whether to use a service or opt in to having your data collected without a clear picture of what you're agreeing to? How would you even know you need to file for a deletion request or that your safety might be compromised, if you don't even have specifics about what data is being collected about you, and where it's going?

It is obvious that industry wrote and negotiated for this amendment, because it allows them to operate with basically no transparency or accountability to people (consumers).

Both California's CCPA/CPRA law and the EU's GDPR require privacy policies to be more specific, and to disclose more detail about the data that are collected and for what purposes its collected. That's good because it helps people (consumers) to make well-informed decisions *before* we sign up for a service or create an account. CA's CPRA even allows people (consumers) to opt out of having their data used in certain automated decisions systems, *and* allows people to disallow selling their data.

Rather than weakening HB 1155's privacy policy and disclosures guidelines, WA should at least be aligning with CA's guideline as a bottom line, or strengthening privacy policies to be even more specific, transparent, and empowering for people's (consumers') privacy.

3. Provides **that a consumer has the right to access the list** of all third parties and affiliates with whom the regulated entity has shared or sold the consumer health data and an email address or other online mechanism for contacting these third parties.
***[NOTE: CORRECTED FROM EARLIER DRAFT - This does not require consumers to do the follow-up on each third party or affiliate ourselves, which is a relief. It's a requirement that info be available to the consumer, via request, because the requirement to provide specifics in privacy policies was removed. That privacy policy change is addressed in (2) above.]

4. Requires a regulated entity to **delete consumer health data within 45 days from authenticating** a consumer's deletion request, **rather than within 30 days of receiving** the request.
[WEAKENS ACCOUNTABILITY & THREATENS SAFETY - EXTENDS TIME]
See analyses of 5. 6. 7. 8. 9. & 10. below.

5. Requires a regulated entity to delete consumer health data from archived and backup systems and **allows the regulated entity up to six months from authenticating** the deletion request to delete data from archived and backup systems.

[EGREGIOUS EXTENSION OF TIME - COMBINED WITH ABOVE AMENDMENTS, THIS MAKES NEARLY A YEAR TO DELETE SOMEONE'S DATA FROM <u>ONE</u> PROVIDER]

See our analysis the rest of our analysis below, *and note* that this intensifies the process burden even further, so that it could actually be legal for companies to take years, *plural*, to follow up on a single consumer deletion request she makes to one entity, because she'll definitely have to then wait for this process to occur with *multiple* entities, and that process, given how widely data is shared and sold, could be *infinite.*

6. ***Allows a regulated entity to not comply*** *with a consumer request* **or to request additional information if the regulated entity is unable to authenticate** the request using commercially reasonable efforts.

[COULD BE A BAD LOOPHOLE?]

Please see the analysis of number one (1), "authentication" above.
In combination with the analysis of the newly added "Authentication" definition to the sub bill, it should be pretty clear that this is a loophole that will allow companies to get away with poor or no accountability and unfair/inequitable business practices, *as well as enable them hold onto data (while actively sharing it).*

It may also allow time for a conservative anti-abortion business owner or employee to alert law enforcement of a deletion request, and then allow time for an exploratory warrant to be filed for access to that person's data. It's a well-known fact that law enforcement agencies have filed disingenuous warrants under the guise of suspecting a drug or other serious offense in order to gain access to information that is then not allowed to be deleted once it is on police servers, and must be retained in accordance with criminal records laws. Civil rights lawyers will confirm: this is a known practice and route for police to steadily collect large amounts of data on targeted individuals and communities, accumulating records and files on people which can be harmful in various ways, and which can then be shared with federal agents or other government entities via inter-local and interagency agreements. It is a shady practice that allows law enforcement to create the appearance of wrong-doing by an individual or group simply on the basis that a LE officer has opened, or requested to open, a case. *There is no reason to believe this shady practice is not, nor will be, exploited by far-right actors in our own or other states to build criminal records data on, and hunt down abortion and gender-affirming care seekers.*

7. Requires a regulated entity to provide requested information in response to a consumer **free of charge, up to twice annually.**

[MAJOR CHANGE: MORE OBSTRUCTION THAN PROTECTION + PAY-FOR-PRIVACY]

This is just terrible. As explained in number 3 above, the data industry is not the credit reporting industry, and they should not be compared. Yet, this change creates a pay-for-privacy norm which creates an inappropriate and totally misapplied legal framing in which people are obligated to share our data with companies (rather than their responsibility to obtain our express, non-coerced, opt-in consent in order to collect it), and in which people must go through onerous and lengthy processes in oder to review and/or delete our own data.

This is just horrifying, it's all wrong, and we can't hate on it enough. **Regardless of whether other privacy laws have this kind of structure, WA should not fall into that trap.**

Big credit companies and other credit business *are data brokers themselves*. In addition, the credit industry is RIFE with data privacy problems, lack of transparency and accountability, and a ton of non-transparent algorithmic and commercial data surveillance harms. Thus, this "free once or twice annually" credit reporting "standard" – which we can say was a valiant but largely unsuccessful attempt to hold the banking and credit industry more accountable to everyday people – should not be the legal basis or standard for creating consumer laws about the massive data flows the credit industry is only one small part of. Regulating the data industry is completely different, far more complex, and we need new data privacy consumer protection standards that actually comprehend and address the scope of the problem, setting both a strong floor on privacy, and creating *people-centered* opt-in and opt-out consumer law. This is even more the case considering that this legislation creates law about a category of data as deeply personal, private and critically sensitive as health data.

My Health My Data stands at the critical intersection of health, privacy, bodily autonomy, gender, reproductive, housing, labor, economic and racial justice; law enforcement abuses *and* broad human rights questions. There is *a lot* going on here.

It's important to consider who this bill is intending to protect, and build from there. We see carveouts and exemptions for industry here, but what about special protections for people being stalked or hunted down by law enforcement for all kinds of health harms? Where are the exemptions and special carveouts for the people fleeing for their lives from abusive situations or people, oppressive religious groups, and government actors who think mental un-wellness, abortion or gender-affirming care vigilantism is their religious or sworn duty? And, what about religious, racial and ethnicity vigilantism that weaponizes health data?

What happens for someone who is being doxxed, stalked or hunted down for accessing a particular kind of healthcare? What happens when a person needs to make repeated requests to delete their data - let's say once a month, or once a week for their safety? Domestic violence & assault survivors, sex workers, people who have been stalked, and people needing to access abortion and gender-affirming care are not on an "every six months I can attempt to be vigilant about my safety" kind of schedule. For too many, the need to secure safety and security are constant. That is the reality *many* have faced for years, and that even more are facing post-Roe.

Rather than creating a burdensome and difficult process people have to go through to protect OUR OWN DATA *AFTER* IT IS OUT OF OUR GRASPS, we need the right to simply decide *not to opt in to sharing it whenever it doesn't feel OK for us.* Period. And that *should* include "de-identified" data.

It's really that simple. It prevents so many harms. As previous testifiers on prior privacy bills in WA State have pointed out (and **I'll take that metaphor a lot further here, A story**): it's the difference between being able to secure your privacy by locking a door and closing windows and curtains, when a data collector comes knocking - "I'd rather not opt-in to you taking my data, thanks!" versus being first forced to open your door, allow a full inspection, documentation, and cataloguing of yourself and pretty much everything inside, which is then

shared with whoever the intruders invite to the estate sale they host in *your* house; and then having those folks who the intruders invited just go right ahead and (because, you know, why not? It's good money right?) invite themselves and even more companies to set up an ongoing *yard* sale outside, with exact replicas of you and everything in your house (each seller with their own table or trunk, though), *and also all of the new things* that enter your house or occur in your house. Because you're forced to just leave those windows and doors open to even participate in modern life, so there's really just a *flow* of information about you and everything in your house going on with these intruders and their estate sale friends now. Until, you discover this isn't safe for you. You'll try and get the whole data-collecting swarm of intruders out. You'll also attempt to boot their friends out of your yard, but *first* you'll have to figure out how to reach them to tell them that - and it was never a well-organized or regular crowd of sellers in the first place, like you never even know explicitly who was there -- some regulars, some popped by with a table once or twice, some just left a tracker... So. you're left desperately try to hunt down literally everywhere everything went, attempt to reclaim it, as well where the copies of the copies of the copies of everything going everywhere went... And you cannot do it. ***The end.***

We're *really* in a pretty intense and deep mess of data sales and sharing.
We MUST pass strong laws now that enable us to tell collectors: delete my info. Make all your friends delete it too. Laws that allow us to simply keep our doors, windows and curtains closed to nosy businessmen and law enforcement snoops, and just say, "No thank you! You're not welcome to my life. I am not opting-in to you collecting and sharing/selling my info."

This law, while it is a *health* data privacy law, and not a *comprehensive* data privacy law, needs to take protections as far is it possibly can. Unfortunately it's unlikely that we'll see de-identified data protected in this law, but that doesn't mean we shouldn't talk about the fact that it is a major loophole and problem in any data privacy bill that offers a blanket exemption for de-identified data.

8. Requires a regulated entity to **respond to consumer requests within 45 days of receiving the request and permits an additional 45-day extension** when reasonably necessary.

[WEAKENS/INTERFERES W/ PROTECTION BY LENGTHENING TIME]

Objections to extension of time for review and deletion requests have already been stated above. So, this is one of a group of changes that creates excessive extension of time and places undue burden on people (the consumer) to attempt to track and follow up on their requests of companies.
Please see issues/analysis of the above items: 1. Authentication 2. Non-transparent privacy policies 4. Unduly extending time 5. Unduly extending time 6. Allowing non-compliance with requests, 7. Restricts access to deletion (pay-for-privacy).

9. Permits the regulated entity to decline to act on a request **or to charge the consumer a reasonable fee** to cover the administrative cost of manifestly unfounded, excessive, or repetitive requests.

[PAY FOR PRIVACY - BAD FOR PEOPLE (CONSUMERS)]

While this could be valid in a few cases, like someone creating a "bot" to file automatic deletion requests over and over; using that possibility as the justification for shuffling the burden of excessive red-tape for deletion, AND fees onto people is not OK. As we've stated above. If companies want to minimize how much they need to communicate with people (consumers) about our data, they should be minimizing what they need to collect, and creating opt-in frameworks for collecting it in the first place.

If companies don't collect, store, share and sell so much data, they don't have to deal with as many deletion requests.

If the Attorney General's Office can't or won't adjust their perspective on this, some ideas:
- Can we get this further defined and more people-friendly, and free of fees for deletion?
- Can we defer to *people's* judgement about how often deletion may be needed, rather than the preferences of tech industry or businesses (which let's be honest, would be *never*)?
- What is a frequency that people feel is reasonable for our safety and security in a post-Roe environment?
- Monthly? What if you travel for an abortion? Weekly?
- For a person seeking safety from a stalker, law enforcement in another state, or other personal threat, being able to request deletion (or even pause or end collection) at any time -- particularly of location data -- could be absolutely critical.

This bill, with this amendment, doesn't address that harm.
But... that's exactly the kind of harm this bill was *supposed* to address, right?

10. Requires a regulated entity to establish a process for a **consumer to appeal the regulated entity's refusal to take action on a request.**

[WEAKENS CONSUMER PROTECTIONS - UNDUE BURDEN ON CONSUMER.]

Again, combined with the above consumer process amendments, this mires people in yet more burdensome process to the point where the "protections" this bill offers are essentially made moot. Please see comments above re data industry. No need to restate the last several pages of analysis.

CUMULATIVE EFFECT OF ITEMS 3. -- 10. ABOVE:
What we don't like about these amendments is the combined cumulative effect they have. We feel like these create inequity and don't alleviate consumers' stress, expense, access issues, process burden, or need for timeliness, particularly in cases of urgent need for deletion.

The combined with the other changes here, mean that a company can

- take 90 days just to respond to a request, (maybe more, due to new req's for authentication, allowed extensions, refusals, consumer appeals and the companies responses...)
- then have an additional *undefined amount of time* to "authenticate" the requestor's identity (when all that may have been required was an email - we've pointed out the many problems with authentication above),
- *after which the company can then take 45 days* to delete any data they have, and then they *can take up to 6 months to track down and delete data from remote servers*, and
- *then,* it may be the consumer's responsibility to follow up in the same prohibitive (or perhaps way more prohibitive - depending who the affiliates owners are and their political agendas) and time-inefficient ways with untold numbers of companies and third parties our data has been sold to or shared with to ensure that their data has in fact been deleted.

The big-data industry is not akin to the credit industry. It's not like there are three big agencies to call. *There are hundreds.* So, trying to have one's data deleted may be an ongoing activity that has no clear end date. It may depend on whether data is shared in discreet batches or is live-syncing across platforms and servers – requiring that people (consumers) understand these differences in data flows *and* know how to ask the appropriate questions of regulated entities and third parties and affiliates about our data (because remember, in the sub bill, privacy policies no longer have to be specific), without knowing anything about how much, or exactly which data was shared with the initial collecting company. And that leaves no way for people (consumers) to prioritize which parties to contact first, or even understand how to make these requests, making it basically impossible for a person (consumer) to ever actually or completely have any control whatsoever over her health data.

So, protections for reproductive and gender-affirming care data? Not so sure about that.

11. Removes the prohibition on sale of consumer health data and instead prohibits selling or offering for sale consumer health data without a valid authorization that meets specified requirements, including a statement that the provision of goods or services may not be conditioned on the consumer signing the valid authorization.

[SO... UNABLE TO SECURE OUR PROTECTION FROM DATA SALES? ACTUALLY... IF THERE IS WILL, WE *DO* HAVE A WAY!]

We understand that this prohibition was removed due concern that prohibiting the sale of data creates a constitutional issue of government overstep into the matters of non-government (commercial) entities expressing or sharing information. Still, that can't be an excuse for simply removing all protections.

This is all the more reason why the other protections in this bill are extremely important to repair.

WA Lawmakers may not be able to ban the sale of consumer health data altogether, but they CAN afford people the right not to opt-in to the sale of our health data, and to opt-out of certain uses of our health data, and to disallow collection, sharing and selling of all of our other data that is collected alongside our health data.

We'd like to see the WA Legislature *protect people's (consumers') rights* to use healthcare services AND stipulate that our health data cannot be sold. Wa Leg can get that done, and this bill can be that vehicle. It's a simple amendment.

12. Modifies the geofencing prohibition to provide that it is unlawful to implement a geofence to identify, track, or collect data from a consumer *that enters* any entity that provides in-person health care services (rather than prohibiting geofencing around any entity that provides in-person health care services in order to identify, track, or collect data from a consumer).

[NARROWS & POSSIBLY NULLIFIES LOCATION PROTECTIONS]
This is a tricky change, and a good example of a small change possibly *significantly* altering or removing a protection in a manner that is difficult to detect on a quick scan, and even difficult to puzzle out on a second read. I'm going to zoom out and just paraphrase these definitions into regular-speak to try and clarify.

This change took a really strong protection in the original bill definition, which defined the unlawful activity as the of creation of a geofence around a physical place:

> **Unlawful to implement a geofence around a clinic** in a way that would be able to identify, track people, collect our health data or send us any notifications or messages because of that geo fence (basically a full-on prohibition of geo-fencing around a clinic).

and replaced it with language that now seems to tie the unlawful activity of creating a geofence to tracking a person (consumer), thus morphing the prohibition into something a lot more nebulous and dubious and possibly nonsensical:

> **Unlawful to implement *a geofence that tracks/identifies/notifies/messages a person (consumer) <u>that</u> <u>enters</u>* a clinic**. (so, a tricky prohibition that only prohibits a geofence used to track a person *if* a person *enters*? Like... What?)

In addition, remember that the sub bill also changed the definition of "geofence" in tandem with this, so the definition now reads: "For purposes of this definition, "geofence" means *a* "*virtual boundary that is 2,000 feet or less <u>from the perimeter</u> of* the physical location."

So, this is also pretty confusing, right? We go from, 'hey, no one can make a geofence around health care facilities if those geofences are used to do X'
to 'no one can make a geofence used to do X that tracks people *that enter* healthcare facilities' and also only if the geofence is 2,000 feet or less *from* the perimeter.
So, is the prohibited geofence activity inside or outside the perimeter of a clinic? Is this a math story problem where the answer is D) none of the above? This is troublingly unclear language.

The original bill definition and prohibition were very clear and straightforward. Easy to understand what was and was not protected.

To say the least, in the sub bill, this protection is now *suuuper-squishy* and muddled. To say a bit more: perhaps this protection has basically been nuanced into thin air by this unclear language?

If you were trying to bring suit alleging your rights under the geofence section of this law had been violated, could you? How would you collect the evidence of that? Or might your lawyer perhaps end up scratching their head and muttering... umm, hmmm... this is... well, hmmm... what a mess!
For the more visually inclined, a chart:

WA People's Privacy - Comparison Chart for Geofencing - My Health My Data HB 1155

MHMD	Orginal Bill	Subsitute Bill
	Section 2 (3)	Section 2 (3)
SAME	With this act (page 2) "...and making it unlawful to utilize a geofence around a facility that provides health care services."	With this act (page 2) "...making it unlawful to utilize a geofence around a facility that provides health care services."
	DEFINITION: (13)	DEFINITION: (14)
SUB BILL ADDS WIERD CARVE-OUT	"Geofence" means technology that uses global positioning coordinates, cell tower connectivity, cellular data, radio frequency identification, Wifi data, and/or any other form of location detection to establish a virtual boundary around a specific physical location.	"Geofence" means technology that uses global positioning coordinates, cell tower connectivity, cellular data, radio frequency identification, Wifi data, and/or any other form of location detection to establish a virtual boundary around a specific physical location. For purposes of this definition, "geofence" means a virtual boundary that is 2,000 feet or less from the perimeter of the physical location.
	Sec. 10.	Sec. 10.
SUB BILL GETS FUZZY	It is unlawful for any person to implement a geofence around any entity that provides in-person health care services where such geofence is used to identify, track, collect data from, or send notifications or messages to a consumer that enters the virtual perimeter.	It is unlawful for any person to implement a geofence to identify, track, collect data from, or send notifications or messages to a consumer that enters any entity that provides in-person health care services.

And, for quick reference, here is a recent article about law enforcement use of geo-fences.

13. Adds exemptions for personal information collected, used, or disclosed in compliance with specified state and federal laws governing human subjects research, quality improvement and peer review committees, reporting of health care-related infections and adverse events, and health care information de-identified in accordance with the HIPAA standards.

[VERY LONG & BROAD LIST OF RESEARCH EXEMPTIONS]

This exemption necessitates a deeper dive into laws governing research than we (sadly) have had time and capacity for this week. Thus, it would be necessary to consult with experts on this subject to fully understand and clarify, but here are a few concerns that immediately jump out with the introduction of this very long list of research exemptions.

Future tech:
Currently we're seeing a huge amount of investment in AI, robotics, biometric and genetic, machine learning and language model research. A lot of this is for military and gov. contractors.

Conscientious objections:
WA People's Privacy takes the firm position that people need to have the right to disallow our data from being collected and used for research and/or to build tools that may be used against humanity, including for purposes of policing, behavioral or personality or risk-scoring, predictive algorithms, intelligence, and military/war applications.

We are concerned that blanket research exemptions may remove *OUR* constitutional rights to speech in these matters. There are many people who do not want our data used for anything involving war, militarism and law enforcement surveillance. In an era wherein war is increasingly virtual, we should ensure the ability of people to withhold our participation via our health data as a critical right.

14. Adds exemptions for personal information collected, used, or disclosed pursuant to the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, the Family Educational Rights and Privacy Act, state law governing Washington Health Benefits Exchange and Statewide Health Care Claims Database, and privacy rules adopted by the Office of the Insurance Commissioner.

[A GRAB-BAG OF EXEMPTIONS FOR WA PROGRAMS, THE WA INSURANCE COMMISSIONER AND FEDERAL LAWS]

More time for deep review of this is needed, but I don't want to hold on releasing this bill analysis, given the time constraints of the legislative session.
Some initial questions here (please do forgive if any of these are moot, or sniffing up any misunderstood trees):

- Seeking clarity regarding any companies/third parties/"processors" that provide services or contract with non-regulated entities in this list: if they are completely exempted, does this also exempt all of the collection, sales and sharing of those processors that serve these non-regulated entities, as well as all of their data flows and interactions?

This is particularly a concern with the WA Health benefits exchange, in the event that this exemption would mean that any and all private entities engaging with health data via the exchange were completely exempted from following this law.

- Seeking clarity regarding any differences in protection where WA's law may actually be stronger, and there is not a conflict of laws.
- Seeking clarity regarding the definitions of "personal information" in the laws in this list, the definition of "consumer health data" in WA's law, and whether, and if so, which "consumer health data" covered in WA's HB 1155/SN5351 is considered "personal information" in these other laws.

Is the distinction clear? Are there overlaps in the definitions of personal information, health data, and biometric data that would disadvantage WA residents if this blanket exemption is added, particularly for laws where there is no conflict nor a federal preemption?

Conclusion

Hopefully, this bill analysis has been informative journey and will be helpful. Writing it has taken weeks and has been a real labor of love.

We have not done any of this work on a salary. We have not had any foundation support. We were not performing this work for funders or trying to protect relationships with anyone in power while doing this work. This is people's self-advocacy.

This is direct democratic engagement for ourselves, our trans lovers, siblings and queer family; for our amigxs, sisters, mothers, grandmothers, aunties/tias, comadres and all of *their* loved ones, too. **This work has been for all of us whom are fighting and absolutely furious, while simultaneously grieving deeply** for the fact that with Roe's overturn, poor women and communities are facing even more entrenched generational poverty and compounding trauma; that our trans community and family members – who already face the world with a kind of courage that cis-gender people can hardly begin to fathom, and are fighting for their lives every single day in this world – are now facing even greater threats; for the fact that people will be forced to birth babies against their will; for the fact that increasing numbers of people will have our bodies weaponized against us as though we are criminals simply for exercising our human right to bodily autonomy; for the fact that many more people will lose their jobs, housing, education, freedoms and even their lives over this; *and for the critical truth that most of these people will be young, poor, black, brown, Indigenous and/or immigrants.*

To be honest, balancing the weight of all that while working on this analysis has been a lot. The stakes are really high here. This bill will impact people's whole entire lives. This is so much heavier than these bits and pieces of industry accountability. We're talking about people's safety and freedom. Nearly all of these amendments in the Substitute House Bill (SHB) 1155 weaken this bill. Why? Because they allow current harms to continue and/or in some cases amplify and create new harms.

To the much-appreciated bill sponsors Sen. Dhingra and Rep. Slatter, Attorney General Ferguson and AGO Staff, and lawmakers we are respectfully asking:

Please ensure that, excepting definition changes 1(C), (F) and (H) and amendment 11. (referring to the numbers in *this* document, not bill), that the bad amendments in the sub bill are swiftly reversed, and that the bill is even *strengthened* from its original form, if possible.

We strongly entreat WA lawmakers to listen to those with experience in understanding both the complexity of data flows and commercial data processes, and our current and future data privacy harms, rather than moneyed interests.

WA has the opportunity to pass the strongest consumer data privacy bill on health data out there. WA prides itself on leading the way, and we can actually *do that* on health data. So, let's pass an unprecedented bill with the intended consequences of reigning in the abuses and harms of the data industry.

People definitely support our lawmakers in doing that. Your re-election campaigns will not be in danger for protecting people's health data. People want privacy.

We're in the midst of a major health data crisis, and on the cusp of health data abuses and harms so egregious, and some so high-tech, it would take another 50-page document to fully explain these. The data industry has gone unregulated for far too long, so now is not only a perfect time for all of our lawmakers to unite on this issue, but it is frankly their duty to do so in a way that is *genuine and real*, and that *provides heretofore unprecedented protections, because post-Roe, we are in unprecedented times.*

Industry lobbyists are unfortunately managing to convince lawmakers there are certain business standards they just have to follow.

that

But just isn't true.

The truth is that the only standards here have been a "wild west" of data flows that are actively placing people in harms way, and that are created by the industry, *for* the industry.

We entreat our lawmakers: please put people first. We're already *way* behind, and the threats – like the overturn of Roe and the war on gender-affirming care – will just keep ballooning.
We can provide people critically needed protections *in the form of the original MY Health My Data bill, and the strengthening changes we've requested.*

We have the chance to make history. To *truly, actually* and *definitively* defend our rights to bodily autonomy via a bulletproof health data privacy bill.

Please, let's not miss this chance!

Thanks in advance for your courage.

~Maya
Founder, WA People's Privacy