February 25, 2022

Hon. Chair Ormbsy
Hon. Ranking Member Stokesbary
Washington State House Appropriations Committee
416 Snyder Ave SW
Olympia, WA 98504

RE: Oppose SB 5534 – Verifiable Credentials

Dear Chair Ormbsy, Ranking Member Stokesbary, and Members of the Committee,

We, the Tech Equity Coalition, alongside organizations representing diverse communities throughout Washington State, urge the Legislature to *oppose* SB 5534, which would direct Washington State to identify uses and create a trust framework for verifiable credentials.

We are extremely concerned that the state is rushing to develop a digital identification framework without adequate consideration of both privacy and equity concerns. Poorly constructed digital identity systems can invade our privacy and other civil liberties, drastically increase social inequities, and cause disproportionate harm to immigrants, communities of color, and people who are especially vulnerable to abuse by police.

We worry that this bill is a step towards creating a mandatory national identification system, something the ACLU and many other civil rights and privacy organizations have strongly opposed for many years.[1] Such systems, especially if linked with other databases, would facilitate widespread government surveillance and substantially infringe upon our privacy rights by painting an intimate picture about where we go, who we talk with, how we worship, and where we stand on political issues. While proposals to establish national identification systems have arisen in various forms over the years, such as a uniform driver's license system and the E-Verify national employment database, they all suffer from the same flaws: They would be ineffective, would provide new avenues for racial and ethnic profiling, and would create a system of internal passports that threaten our privacy and civil liberties.

In many countries, such as Argentina, national ID regimes have been adopted during military or authoritarian regimes, because they increase the power of authorities to reduce people's freedoms to those granted by the ID.[2]

We are also very concerned that the bill's support comes primarily from blockchain companies and consortia to promote the growth of blockchain. The privacy, security, and equity impacts of having people's identities stored and shared using blockchain-based technology have not been adequately explored, and the Legislature should not direct the State to use a specific technology without carefully considering both the short and long-term effects of such use. In fact, a verifiable credential system does not require the use of blockchain technology at all.

---

[1] 5 Problems with National ID Cards | American Civil Liberties Union (aclu.org)
[2] Biometrics in Argentina: Mass Surveillance as a State Policy | Electronic Frontier Foundation (eff.org)

As the Electronic Frontier Foundation asserted in their opposition[3] in 2020 to a digital verifiable credential bill in California:

"[B]lockchain verified credentials would make it a normal practice for people to present a digital token as a condition to entering a physical space, and for gatekeepers—such as security guards or law enforcement officers—to demand such digital tokens. Such a system could be expanded to document not just a medical test result, but also every occasion when the subject presented that result to a gatekeeper. It could also be expanded to serve as a verified credential of any other bit of personal information that might be relevant to a gatekeeper, such as age, pregnancy, or HIV status. And all of the personal information associated with a blockchain verified credential could be linked to other digital record-keeping systems."

Today, Washington agencies use a number of systems that have not been adequately assessed for errors, biases, and vulnerabilities. For example, we recently learned about the Department of Licensing's recent data breach, affecting 650,000 licensed professionals and business owners. This bill puts agencies, that have not yet ensured that existing systems are secure, in charge of developing an ambitious trust framework. This approach is ill-timed. Agencies should focus first on addressing the existing security, privacy, and bias problems instead of creating a new system that will likely poses many new risks and challenges.

Finally, the bill prioritizes tech industry perspectives, rather than Washingtonians' needs. While tech industry perspectives are important, they are insufficient. Trade associations represent the interests of their members, and not those of the general public. It is critical that the work to consider a verifiable credential system be done with a much broader range of stakeholders, including people representing communities historically affected by bias in technology. It is the public that will be using these new systems, so it is vital to include these perspectives.

It is clear there must be much more careful consideration and community engagement on this issue. Washington State should not imprudently jump ahead to develop a trust framework that could harm the privacy and civil liberties of all Washingtonians, and especially those of the most marginalized communities. We have learned from lessons in India[4] and Kenya[5] that rushing ahead to create digital ID systems can cause serious harms that are extremely difficult to retroactively fix.[6]

We urge lawmakers to oppose SB 5534.

Signed,
ACLU of Washington
Coalition of Seattle Indian Americans
Densho
Indivisible Bainbridge Island

---

[3] No to California Bill on Verified Credentials of COVID-19 Test Results | Electronic Frontier Foundation (eff.org)
[4] You can't make citizens safer by making them more vulnerable. Aadhaar does exactly that (indiatimes.com)
[5] Kenya's New Digital IDs May Exclude Millions of Minorities - The New York Times (nytimes.com)
[6] By embracing blockchain, a California bill takes the wrong step forward. - Open Policy & Advocacy (mozilla.org)

Indivisible Bellingham
Indivisible Plus Washington
John T. Williams Organizing Committee
La Resistencia
MAPS-AMEN (American Muslim Empowerment Network)
Parent Coalition for Student Privacy
People First Bellingham
Snohomish County Indivisible
WA People's Privacy Network
WA Poor People's Campaign
Wallingford Indivisible