

March 31, 2026

To the Chair and Members of the Senate Committee on A.I. and Emerging Technology,

My name is Angel Lopez, and I am a resident of Providence. I write to you today in opposition to Senate Bill 2638 because the proposed changes move away from the specifics included within the exiting legislation, instead of zooming in to focus on the new and very private personal data that is being gathered and processed today.

A cyber security plan is as clear as a disaster recovery plan. This bill will remove the terms "classified data" and "personal data" and merge the two distinct definitions into the term Personally Identifiable Information. The distinct categories that make up "classified data" require industry standard encryption to protect from identity theft. The combination of data sets that define "personal data" require additional in person human awareness, and policy to ensure the adequate amount of security and precaution is present to protect client data. When both these definitions are squeezed into Personally Identifiable Information the distinction between the two are invisible.

In addition, the bill also includes biometric data and internet data within the definition of Personally Identifiable Information. I would say that descriptive elements of both biometric data and internet data can be categorized as either "classified" or "personal data." This legislation adds two new and distinct data sets into a Gumbo of Personally Identifiable Information, allowing previously included and added information to simmer inside the same pot of definition (10) "reasonable security procedures".

Is there a known best practice to protect biometric data? Is the best practice more robust for a fingerprint than for a typing pattern? How will that standard be upheld when biometric data is grouped together with internet data? Should certain aspects of biometric data require a higher level of encryption in 2026 than classified tax information? There must be a clear separation of data sets and any process that involves a combination of data sets must have reasonable layers of encryption, human intervention, and awareness to ensure the identity protection of the client or consumer during a time of elevated risk.

After the "RIBridges" data breach, this state requires a robust Identity Theft Protect Act. The Act must provide clarity and be updated to reference the new data being processed and mention reasonable or industry standards of encryption for each data category. This bill as written is

Angel's Testimony in Opposition to Senate Bill 2638

protecting the trade secrets of the “controllers” as described in the RI Data Transparency and Protection Act and not the residents and consumers in Rhode Island. Please hold Senate Bill 2638.

Thank you for taking the time to read this.

Angel Lopez
Resident of Providence, RI