STATE PRIVACY & SECURITY COALITION

January 13, 2025

The Honorable Bob Lynn, Chair
The Honorable Dennis Mannion, Vice Chair
House Judiciary Committee
The General Court of New Hampshire
107 North Main Street
Concord, NH 03301

RE: HB 1436 - Common Law Privacy and Consumer Protection Act

Dear Chair Lynn, Vice Chair Mannion, and Members of the Committee:

The State Privacy & Security Coalition (SPSC), representing over 30 companies and seven trade associations across the retail, telecommunications, technology, automotive, healthcare, and payment card sectors, appreciates the opportunity to provide testimony on House Bill 1436.

New Hampshire recently enacted a comprehensive privacy law, RSA 507-H. For this reason, we must respectfully oppose HB 1436 because it would undermine the comprehensive law. That statute, which took effect on January 1, 2025, establishes a rights-based framework that gives consumers meaningful control over their personal data, while imposing clear and enforceable obligations on the businesses that collect and process such data. Those protections are enforced by the New Hampshire Attorney General.

Moreover, RSA 507-H was crafted to align with the national privacy framework that has now been adopted across two other New England states and in fifteen additional states nationwide. That model protects the data rights of more than 100 million Americans while allowing businesses to operate across state lines under consistent rules. HB 1436 does not build on that framework. Instead, it would undermine it with an untested legal regime based on property ownership and common-law bailment, introducing conflict into a system that is only just beginning to take effect.

I. HB 1436 UNDERMINES NEW HAMPSHIRE'S RIGHTS-BASED PRIVACY LAW WITH A PROPERTY-LAW BASED FRAMEWORK

RSA 507-H is built on a rights-and-responsibilities model that gives consumers meaningful control over their data while permitting processing for legitimate purposes. Consumers have rights to access, correct, delete, port, and opt out of certain uses of their personal data, and controllers must limit collection to what is adequate, relevant, and reasonably necessary, process data only for compatible purposes, and maintain appropriate safeguards. *See* N.H. Rev. Stat. Ann. §§ 507-H:4, 507-H:6. In contrast, HB 1436 declares that personal information "remains the property of its original owner" even after being incorporated into digital records. That shift fundamentally alters the structure of privacy law in New Hampshire by substituting a regime of ownership, possession, and control drawn from property law for a system based on rights, duties, and accountability.

Importantly, property law brings with it doctrines such as trespass, conversion, and replevin that were developed for ***interests attached to physical property***.[1] Those doctrines do not translate to modern data processing, which necessarily requires copying, transmitting, encrypting, backing up, and analyzing personal information for digital services to function. Under HB 1436, routine activities expressly permitted under RSA 507-H, including fraud detection, cybersecurity monitoring, product improvement, and compliance with legal obligations, could be recast as unauthorized interference with an individual's asserted property interest. The result would be two overlapping and inconsistent legal standards governing the same data, leaving businesses uncertain about compliance and consumers unclear about their rights.

[1] *See Trespass*, *The Law Dictionary*, https://thelawdictionary.org/trespass/ (last visited Jan. 12, 2026) (defining trespass, "[i]n strictest sense, [as] an entry on another's ground, without a lawful authority, and doing some damage, however inconsiderable, to his real property."); *Conversion*, *The Law Dictionary*, https://thelawdictionary.org/conversion/ (last visited Jan. 12, 2026) (defining conversion as an unauthorized act that deprives an owner of property); *Replevin*, *The Law Dictionary*, https://thelawdictionary.org/replevin/ (last visited Jan. 12, 2026) (defining replevin as the common-law action to recover personal property wrongfully taken or detained).

II. THE BILL'S BAILMENT PRESUMPTION IS INCOMPATIBLE WITH CLOUD COMPUTING

HB 1436 goes further by presuming that when a person's unpublished personal information is placed into a digital record or cloud server, a bailment for mutual benefit is created. Bailment is a doctrine rooted in ***physical custody***, where one party (i.e., "bailor") temporarily transfers possession of a specific and identifiable object to another (i.e., "bailee") with the expectation that the same object will later be returned.[2] That legal model does not align with how digital information is created, stored, or processed.

In modern cloud environments, personal data is not conveyed as a single object. It is copied, encrypted, cached, transformed, and stored redundantly across multiple systems and locations. Multiple processors, subcontractors, and automated systems may access and process the same data simultaneously in order to deliver the service the consumer requested. In that environment, concepts such as exclusive possession, return of the identical item, or loss of a particular object have no logical application.

RSA 507-H already regulates these realities through a modern statutory framework. The law assigns responsibility through controller–processor relationships, requires contracts governing data handling, imposes confidentiality and security obligations, and mandates deletion or retention of data at the end of a service relationship where appropriate. Those rules are designed to protect personal data across distributed digital platforms without relying on physical custody concepts.

For instance, a consumer who uses a healthcare or fitness tracking app has personal data stored with a cloud provider. Under RSA 507-H, the app provider remains the controller of the data, the cloud provider is a processor, and their contract governs how the data is stored, secured, and deleted. If the consumer closes the account, the controller must ensure the data is deleted or retained only as legally required, and the processor must follow those instructions.

Under HB 1436, that same arrangement becomes a presumed bailment of the consumer's "property." The cloud provider would be deemed to possess the consumer's personal data as a bailee, even though the data exists simultaneously in encrypted backups, mirrored servers, and system logs. If any copy remains for cybersecurity or legal compliance, a consumer could claim that the "property" was not returned, exposing companies to bailment liability even when they fully complied with RSA 507-H and their contractual obligations.

By inserting bailment into the state's comprehensive privacy statute, HB 1436 replaces workable and technology-neutral privacy rules with legal doctrines that cannot be meaningfully applied to cloud-based data.

III. HB 1436 CREATES AN UNWORKABLE ENFORCEMENT REGIME

RSA 507-H gives the New Hampshire Attorney General clear authority to enforce modern privacy standards governing how companies collect, use, and safeguard personal data. In furtherance of that role, the Attorney General's Office has joined the *Consortium of Privacy Regulators*, a bipartisan coalition of state regulators that coordinates expertise and enforcement across states with ***aligned*** privacy laws.[3]

HB 1436 would redirect that enforcement function toward property and bailment disputes. Instead of evaluating compliance with privacy obligations similar to other states, the Attorney General would be required to litigate questions of ownership and possession of digital information. The bill's fiscal note confirms that additional investigators and attorneys would be needed to carry out these new enforcement responsibilities. Accordingly, this change diverts limited enforcement resources away from protecting consumers and toward resolving complex and unsettled questions of property law. RSA 507-H was designed to support efficient, targeted, and effective privacy enforcement. HB

[2] *See Bailment*, *The Law Dictionary*, https://thelawdictionary.org/bailment/ (last visited Jan. 12, 2026) (defining bailment as a relationship in which physical possession of personal property is transferred from one person to another for a particular purpose).

[3] *See New Hampshire Joins Bipartisan Consortium of Privacy Regulators to Collaborate on Data Privacy Enforcement*, N.H. DEP'T OF JUSTICE (Oct. 8, 2025), https://www.doj.nh.gov/news-and-media/new-hampshire-joins-bipartisan-consortium-privacy-regulators-collaborate-data.

1436 would undermine that goal by replacing a clear regulatory framework with a more cumbersome and less predictable enforcement regime.

* * *

For these reasons, we respectfully urge the Committee not to advance HB 1436. New Hampshire has already enacted a comprehensive privacy law that establishes clear consumer rights, consistent standards for businesses, and centralized enforcement by the Attorney General. Creating a parallel legal framework based on property and bailment concepts is unnecessary and would introduce confusion for consumers, inconsistency for businesses, and added complexity for regulators charged with enforcing privacy protections.

We appreciate the time and energy your office has put into this legislation and thank you for your consideration of our comments. Please do not hesitate to contact us with any questions or concerns.

Respectfully submitted,

Andrew A. Kingman
Counsel, State Privacy & Security Coalition

William C. Martinez
Counsel, State Privacy & Security Coalition