STATE PRIVACY & SECURITY COALITION

September 25, 2026

The Honorable Chris Rothfuss
The Honorable Daniel Singh
Select Committee on Blockchain, Financial Technology and Digital Innovation Technology
Wyoming State Legislature
200 West 24th Street
Cheyenne, WY 82002

RE: Wyoming Personal Data Ownership Act

Co-Chairs Rothfuss, Singh and Members of the Committee:

The State Privacy & Security Coalition ("SPSC") is a multi-sector coalition representing over 30 companies and seven trade associations across the retail, technology, telecommunications, healthcare, automotive, and payment card sectors. We appreciate the Committee's interest in protecting Wyoming residents' personal data and ensuring that consumers have meaningful control over how their information is collected and used.

SPSC has serious concerns with the approach taken in the Wyoming Personal Data Ownership Act (the "Bill"). Treating personal data as property creates significant legal uncertainty and practical problems that could undermine those goals. These concerns are particularly significant given the unresolved questions identified by the Legislative Service Office ("LSO") throughout the draft. LSO staff cautioned that the Bill "may have unintended consequences" because of "the nuance and complexity of the property and rights at issue," including "legal, operational or practical consequences that cannot be fully identified or anticipated in advance."

As discussed below, these unresolved issues underscore the risks of replacing an established consumer-protection framework with a novel property-rights regime.

I. A COMPREHENSIVE CONSUMER-PROTECTION PRIVACY FRAMEWORK IS THE BETTER APPROACH

The Bill seeks to address legitimate concerns: consumers should understand what personal data is collected about them, how it is used, with whom it is shared, and having meaningful control over that data. These goals do not require treating personal data as property. Each is already addressed through the comprehensive consumer-protection privacy framework adopted by every state that has enacted comprehensive privacy legislation to date, without the legal and practical complications created by a property-rights model.

a. Every Enacted State Privacy Law Uses a Consumer-Protection Framework

Twenty-four states have now enacted comprehensive consumer privacy laws.[1] While these laws differ in their scope and specific requirements, they share the same basic approach: establishing rights for consumers and corresponding obligations for businesses that collect and process personal data. None treat personal data as property or relies on property ownership as the basis for protecting consumers' privacy.

That approach reflects the practical realities of regulating personal data. Privacy laws can give consumers meaningful control over their information without requiring courts, businesses, and consumers to determine who holds legal title to data or how traditional principles of property law apply when the same information may be held, used, or disclosed by multiple parties.

Although the specific rights vary by state, the comprehensive state privacy laws generally give consumers rights to:

- **opt in** to the use of sensitive data, including precise geolocation data, biometric data, and data relating to a known child;
- **know** whether a business is processing their personal data and **access** that data;
- **obtain a copy** of their personal data;
- **correct** inaccurate personal data;
- **delete** personal data; and
- **opt out** of the sale of personal data, targeted advertising, and certain forms of profiling.

These rights address the same core concerns underlying the Bill: transparency, consumer control, and accountability. But they do so through defined statutory rights and corresponding obligations rather than by treating personal data as intangible personal property. A consumer does not need to hold legal "title" to personal data to have a statutory right to access or delete it. The existing consumer-protection model provides Wyoming with an established framework for addressing the Bill's underlying concerns without the confusion and unintended consequences of treating data as intangible personal property.

[1] *See, e.g.*, Cal. Civ. Code §§ 1798.100–1798.199.100; Colo. Rev. Stat. §§ 6-1-1301 to 6-1-1314; Conn. Gen. Stat. §§ 42-515 to 42-525; Md. Code, Com. Law §§ 14-4601 to 14-4614; N.J. Stat. §§ 56:8-166.4 to 56:8-166.19; Or. Rev. Stat. §§ 646A.570–646A.589; Tex. Bus. & Com. Code §§ 541.001–541.205; Va. Code §§ 59.1-575 to 59.1-585.

b. <u>The Comprehensive Privacy Framework Is Interoperable. The Proposed Wyoming Framework Is Not</u>

One of the practical advantages of the existing state privacy framework is interoperability. Although the 24 enacted comprehensive privacy laws differ in certain respects, they generally follow a common structure built around consumer rights, obligations for businesses that process personal data, applicability thresholds and exemptions, and attorney general enforcement. That common structure allows businesses to develop privacy programs that can be adapted across jurisdictions while giving consumers broadly similar protections from state to state.

The Bill departs from that structure in fundamental ways that are not found in any other state data privacy law. Rather than regulating how businesses collect, use, and disclose personal data, it provides that individuals hold a property interest in their personal data and that businesses obtain authority to use that property through licenses. As a result, businesses operating nationally could not simply incorporate Wyoming-specific requirements into the compliance frameworks they already use for other state privacy laws. They would need to account for a separate legal framework governing ownership, licensing, and transfer of personal data regulation.

The differences are not limited to terminology. The Bill takes materially different approaches to several foundational issues addressed by existing comprehensive state privacy laws. For example:

- Existing state privacy laws generally regulate the sale of personal data through consumer rights and business obligations, including opt-out rights; the Bill instead provides that ownership of personal data may not be permanently transferred.

- Existing state privacy laws generally exclude data processed in the employment context or otherwise provide specific treatment for employment-related data; the Bill would bring that data within its property-rights framework.

- Existing state privacy laws generally rely on attorney general enforcement; the Bill creates a private right of action and authorizes statutory damages of up to $15,000 per person.

- Existing state privacy laws generally use applicability thresholds or other limitations to define the businesses subject to their requirements; the Bill does not establish a comparable processing threshold.

These differences would require businesses to treat Wyoming data under a fundamentally different legal framework from data governed by other state privacy laws. A business that may process or sell personal data subject to defined consumer rights elsewhere, for example, would need to determine whether the same activity constitutes an impermissible transfer of a

Wyoming resident's property interest. Similarly, ordinary corporate transactions could raise separate questions about whether existing authority to process Wyoming residents' data survives a change in control.

The practical consequence is fragmentation. Instead of building on the increasingly interoperable framework developed across the states, the Bill would create a separate property and licensing regime that businesses would need to identify, interpret, and administer alongside their existing privacy programs. That divergence would increase compliance complexity and uncertainty without necessarily providing Wyoming residents with greater practical control over their personal data.

II. THE BILL'S PROPERTY-RIGHTS FRAMEWORK CREATES SIGNIFICANT LEGAL AND PRACTICAL UNCERTAINTY

Beyond the structural advantages of the consumer-protection framework, the Bill's property-rights approach raises a series of difficult legal and practical questions. LSO staff identified many of these issues throughout the draft, including questions concerning the inalienability of the property interest the Bill creates, ownership of data relating to more than one person, and personal jurisdiction and due process. LSO staff cautioned that the Bill "may have unintended consequences" given "the nuance and complexity of the property and rights at issue." These concerns reflect the difficulty of applying traditional concepts of property ownership to information that can simultaneously relate to multiple people, be held by multiple entities, and be processed across jurisdictions.

a. <u>The Bill Creates a Property Right While Prohibiting Owners from Transferring It</u>

Section 34-31-104(b) provides that title to personal data "is not alienable, assignable or transferable during the data owner's life" and may pass only "by inheritance or succession." A Wyoming resident, therefore, could not permanently sell, assign, or otherwise transfer title to their personal data, even voluntarily.

LSO staff identified this tension directly, observing that the Bill "appears to prohibit a data owner from permanently selling, assigning, or waiving the data owner's title to personal data or ownership interest in personal data, even if the data owner voluntarily agrees to do so."

That restriction conflicts with a basic right of property ownership: the ability of an owner to transfer what they own. Wyoming courts have long recognized the policy favoring the free alienation of property. *See, e.g.*, *Williams v. Watt*, 668 P.2d 620, 633 (Wyo. 1983) (explaining that "the underlying purpose of the rule [against perpetuities] is to provide for the free alienation of property"); *accord McGinnis v. McGinnis*, 391 P.2d 927, 932–33 (Wyo. 1964); *see also Horse Creek Conservation Dist. v. State ex rel. Wyo. AG*, 2009 WY 143, ¶ 30 (Wyo. 2009) (citing both *Williams* and *McGinnis* and reaffirming that "the rule forbids the protracted suspension of the right to alienate property[.]").

The Bill would create a new property interest while expressly withholding the owner's ability to permanently transfer that property during life. A Wyoming resident would hold "title" to personal data but could not sell, assign, or otherwise transfer that title, regardless of the resident's wishes or the circumstances of the transaction. The result is an unusual form of ownership that gives individuals title to personal data while denying them one of the principal rights ordinarily associated with ownership.

b. <u>The Bill Does Not Explain Who Owns Data That Relates to More Than One Person</u>

The Bill defines a "data owner" as the person to whom data "relates or is linked or reasonably linkable," but does not address what happens when the same information relates to multiple people. LSO staff identified the problem directly, asking "who owns personal data relating to more than one person."

That situation is common. Joint bank accounts, shared smart-home devices, family streaming accounts, household purchases, photographs, communications, and other records can contain information linked to multiple identifiable individuals. If each person has a property interest in the same information, the Bill provides no rules governing the relationship among those interests.

The problem becomes particularly difficult when individuals exercise conflicting rights. One member of a household, for example, could seek deletion of information that another household member seeks to access or preserve. The Bill does not establish a joint-ownership framework, priority rules, or another mechanism for resolving competing claims to the same data.

A consumer-protection framework avoids this threshold ownership problem. It can define who may exercise statutory rights and under what circumstances without requiring courts to determine which individual holds title to information relating to multiple people.

c. <u>Treating Personal Data as Individual Property Creates Unresolved Questions for Marriage and Divorce</u>

The Bill also does not explain how its new property interest interacts with Wyoming law governing marital property and divorce. Personal data is made inalienable during the owner's lifetime and belongs to the individual to whom the information is linked or reasonably linkable. But the Bill does not address whether that interest may constitute marital property, whether a spouse may acquire an interest in it, or how a court should treat the property interest when dissolving a marriage.

The Bill separately regulates access to personal data in civil proceedings. Section 34-31-105(d)(ii) requires a court order, notice to the data owner, and an opportunity for the data

owner to be heard before certain personal data may be obtained in a civil action. That requirement could affect ordinary discovery involving financial accounts and other records containing personal data.

The result is a new layer of uncertainty in proceedings where courts routinely need access to personal and financial information. Rather than simply applying existing rules governing discovery and marital property, courts may first need to determine what rights arise from the Bill's newly created property interest and how those rights interact with existing procedural and substantive law.

d. The Bill Could Reach Information Used in Expressive and Creative Works

The Bill's broad definition of "personal data" also raises questions concerning expressive works. Personal data includes information "linked or reasonably linkable to an identified or identifiable natural person." Photographs, videos, biographies, memoirs, documentaries, and similar works routinely contain information meeting that definition.

The Bill includes exceptions for certain "published personal expression" and "expressive works," but those exceptions are subject to limitations. Among other things, the exceptions do not apply in specified circumstances involving use of a data owner's identity to identify, profile, contact, locate, or make decisions concerning that person, or where processing creates or derives a profile reasonably linkable to the data owner.

Those limitations create uncertainty about where protected expression ends and regulated processing begins. The issue is particularly significant for commercial publications, documentaries, biographical works, and other expressive activities involving information about identifiable individuals. By characterizing the underlying information as another person's property, the Bill introduces property claims into an area already governed by established constitutional, intellectual-property, and state-law protections.

e. Applying the Property Framework to Employment Data Could Interfere with Ordinary Workplace Recordkeeping

The Bill expressly applies its framework to employment-related data and treats employers processing that information as data custodians. That approach differs significantly from the treatment of employment data under the existing state comprehensive privacy framework.

Employers necessarily process substantial amounts of personal data for payroll, benefits administration, performance management, workplace investigations, safety, regulatory compliance, and other routine employment functions. Applying consumer-style access and deletion rights to those records creates practical questions that do not arise when employment data is excluded from a comprehensive consumer privacy statute.

For example, Section 34-31-107(a)(iv) provides a right to "verifiable deletion at any time," subject to the Bill's exceptions. An employee could, therefore, seek deletion of information contained in performance records, disciplinary materials, complaints, or investigation files. Although the Bill contains retention exceptions, including for litigation holds and certain employment-related retention policies, their application may not always be clear, particularly before litigation is anticipated or a personnel action has occurred.

Employers should not be placed in the position of determining whether a newly created property right requires deletion of records they may need for legitimate employment, compliance, or evidentiary purposes. Existing privacy frameworks generally avoid that problem by treating employment information separately from consumer data.

f. The Bill's Extraterritorial Reach Raises Dormant Commerce Clause Questions

The Bill defines "data custodian" to include a person processing a data owner's personal data "regardless of the location of the person or of any direct relationship with the data owner." The provision, therefore, purports to regulate entities outside Wyoming based on their processing of data associated with a Wyoming resident.

That breadth raises questions concerning the constitutional limits on state regulation of interstate commerce. The United States Supreme Court has recognized that the Commerce Clause limits a state's ability to project its regulatory regime beyond its borders. In *Healy v. Beer Institute*, the Court invalidated a Connecticut beer-pricing law whose practical effect was to control commercial activity occurring wholly outside the state, explaining that "the practical effect of the statute must be evaluated not only by considering the consequences of the statute itself, but also by considering how the challenged statute may interact with the legitimate regulatory regimes of other States and what effect would arise if not one, but many or every, State adopted similar legislation." 491 U.S. 324, 336 (1989). The Court emphasized that, "[g]enerally speaking, the Commerce Clause protects against inconsistent legislation arising from the projection of one state regulatory regime into the jurisdiction of another State." *Id*. at 336–37.

The Court has separately recognized that even an evenhanded state law directed toward a legitimate local interest may raise Commerce Clause concerns when its incidental burdens on interstate commerce are excessive in relation to its local benefits. *See Pike v. Bruce Church, Inc.*, 397 U.S. 137, 142 (1970) (holding that a state law will be upheld "unless the burden imposed on such commerce is clearly excessive in relation to the putative local benefits.").

Both principles are relevant here. The Bill defines a "data custodian" without regard to the custodian's location or whether it has a direct relationship with the Wyoming resident, while imposing a property-rights and licensing framework that differs substantially from the privacy frameworks governing the same processing activities in other states. The resulting inquiry is not simply whether the Bill has effects outside Wyoming. Rather, it is whether the Bill would, in

practice, regulate out-of-state data-processing activities or impose substantial burdens on interstate commerce that are disproportionate to Wyoming's legitimate interest in protecting its residents' personal data.

g. <u>The Bill's "Regardless of Location" Standard Also Raises Personal-Jurisdiction and Due-Process Questions</u>

The same provision raises a separate constitutional concern regarding personal jurisdiction. By defining a "data custodian" without regard to the entity's location or the existence of a direct relationship with the data owner, the Bill purports to impose substantive obligations on entities that may have limited, or potentially no purposeful, contacts with Wyoming.

The Due Process Clause, however, limits a state court's authority to exercise jurisdiction over a nonresident defendant. A defendant that is not subject to general jurisdiction in the forum must have "minimum contacts" with the state such that exercising jurisdiction comports with "traditional notions of fair play and substantial justice." *International Shoe Co. v. Washington*, 326 U.S. 310, 316–17 (1945). The Supreme Court has emphasized that this inquiry focuses on contacts created by the defendant itself, not merely the defendant's contacts with a person who happens to reside in the forum. *See Walden v. Fiore*, 571 U.S. 277, 284–86 (2014) (explaining that the minimum-contacts analysis looks to "the defendant's contacts with the forum State itself, not the defendant's contacts with persons who reside there," and that the plaintiff cannot be the defendant's only link to the forum).

For specific jurisdiction, moreover, the defendant must have purposefully established contacts with the forum, and the claims at issue must "arise out of or relate to" those contacts. *See Ford Motor Co. v. Mont. Eighth Jud. Dist. Ct.*, 592 U.S. 351, 359–60 (2021) (explaining that specific jurisdiction requires the defendant to purposefully avail itself of the privilege of conducting activities within the forum and requires a sufficient relationship between the defendant's forum contacts and the claims asserted). These limitations ensure that jurisdiction is based on the defendant's own relationship with the state rather than the "random, isolated, or fortuitous" circumstance that its activities happen to affect a forum resident. *Id.* at 359.

The Bill's definition of "data custodian" does not account for these constitutional limitations. An out-of-state entity could fall within the statutory definition solely because it processes personal data belonging to a Wyoming resident, "regardless of the location of the person or of any direct relationship with the data owner." But the fact that information relates to a Wyoming resident does not, standing alone, establish that the entity purposefully directed activity toward Wyoming or otherwise formed the relationship with the State required for personal jurisdiction.

LSO staff appropriately identified this problem in the draft. A statute may define the entities subject to its substantive requirements, but that definition cannot expand the constitutional jurisdiction of Wyoming courts. As a result, the Bill risks creating obligations and private causes of action against entities that fall within its definition of "data custodian" even though, in

certain circumstances, those entities may lack the minimum contacts necessary to be sued in Wyoming. At minimum, the disconnect between the Bill's "regardless of location" language and constitutional limits on personal jurisdiction creates substantial uncertainty about the reach and enforceability of the statute.

h. <u>The Bill's Broad Private Right of Action Would Significantly Expand Privacy Litigation</u>

The Bill also departs from the prevailing state comprehensive privacy framework by creating a private right of action for violations of its requirements. Section 34-31-117 authorizes private litigation and statutory damages of up to $15,000 per person, while Section 34-31-104(e) provides that unauthorized processing constitutes a legally cognizable injury without proof of physical harm or economic loss.

The combination is significant. It allows litigation based on alleged statutory violations without requiring a plaintiff to establish traditional economic or physical injury and attaches potentially substantial statutory damages to those claims. Combined with the Bill's broad scope and lack of a minimum processing threshold, these provisions could expose businesses of widely varying sizes to significant litigation risk.

That enforcement model differs materially from the approach generally taken in comprehensive state privacy laws, which primarily rely on enforcement by state officials, subject to limited exceptions in particular statutes. Wyoming should carefully consider whether creating a broad private enforcement mechanism advances the Bill's consumer-protection goals or instead creates litigation incentives unrelated to actual consumer harm.

* * *

The Wyoming Personal Data Ownership Act is well-intentioned, but the Bill's property-rights framework creates more legal uncertainty and practical problems than it solves. Wyoming's interests are better served by the proven comprehensive consumer-protection privacy framework that all 24 states with enacted privacy laws have adopted. That framework provides consumers with meaningful, exercisable rights, while giving businesses clear and workable obligations. It avoids the property-law complications the Bill creates and is interoperable with the existing national landscape of state privacy laws.

We appreciate the Committee's time and consideration and stand ready to work collaboratively on privacy legislation that achieves durable, enforceable, and balanced protections for Wyoming residents.

Respectfully submitted,



Andrew A. Kingman
Counsel, State Privacy & Security Coalition



William C. Martinez
Counsel, State Privacy & Security Coalition