ADVANCED INTELLIGENT NETWORKS

P.O. BOX 22551 · CHEYENNE, WYOMING 82003 · 303-309-1432

Issues of Self Sovereign Identification and Data Protection in Wyoming

Prepared for Voir Dire, llc and
The Wyoming Legislature Select Committee on Blockchain, Financial Technology and Digital Innovation Technology

September 22, 2025

Abstract:

As long as permission is needed to participate in society, privacy will not exist.

The Financial Crimes Enforcement Network (FinCEN) requires "**Know Your Customer"** private data collection in order to participate in banking. Is there anyone who believes that your private data is secure and immune to malicious release of data? The betrayal of trust in Government exemplified by rampant lawfare, debanking, and political and social censorship, is a common truth.

That being said, few of us would hesitate to offer information that is part of our private data in order to receive services, prove innocence, or participate in honest legal endeavors. In Whalen v. Roe (1977), the Supreme Court recognized a constitutional right to privacy, including an individual's interest in preventing the disclosure of personal matters. The 4th and 5th Amendments offer protections securing private data and against the forced disclosure of encrypted private matters.

Somewhere in between FinCEN and the Supreme Court is Self Sovereign ID.

The assumption that private data once shared by government requirement, effectively becomes "public" or free of "risk of exposure" raises valid questions about the effectiveness of data protection laws. Under U.S. law (United States v. Miller, 1976; Smith v. Maryland, 1979), data shared with third parties (e.g., banks) loses some Fourth Amendment protections against government searches, as individuals have a reduced expectation of privacy. Even with protections, governments and third parties may suffer breaches, exposing plaintext data.

Wyoming has several statutes that impose requirements on the collection of personal or specific types of data, emphasizing that such collection must serve a defined, legitimate purpose, yet Real-ID makes its demands. Wyoming does not yet have a comprehensive consumer data privacy act.

This paper proposes solutions developed for Voir Dire, LLC, which Wyoming and financial institutions can adopt to authenticate digital credentials, minimize the exposure of collected data, and create non-repudiable digital identities that are controlled by the data owner, rather than granted as government-issued permissions.

1 Introduction

Voir Dire, llc is establishing a decentralized Self Sovereign Identity ESCROW to enable a ***PERSON***‡ to exercise control over a Digital Identity which contains Verified Credentials, financial account keys, medical records, public keys, and network access tokens.

While preparing this report and doing research into Wyoming statutes regarding the proposed law 26LSO-0012, a number of general data processing deficiencies were found. 26LSO-0012 is specifically concerned with the protection, handling, and distribution of personal data that it collects.

1.1 Purpose

The purpose of this document is to review the government of Wyoming data structures that can reveal private data while suggesting changes and process methods that would facilitate a decentralized key escrow self-sovereign ID and information elements that can remedy accidental exposure and provide non-repudiation of required data.

1.2 Scope

Voir Dire can provide targeted self-sovereign identity data using “Zero Knowledge Proofs” to protect financial accounts, digital credentials, and medical and personal records regardless of Wyoming's actions.

1.2.1 Inclusions:

This is meant for states, Wyoming included, who collect private data while leaving pertinent records unprotected. This is meant for those that wish to control and limit exposure of legal private matters against malicious agents that will use that exposed data against the owner or diminish their rights.

1.2.2 Exclusions:

This is not intended to be legal counsel. Solutions provided here may be encumbered by patents or other claims to intellectual property and process. Regardless of Wyoming's actions, there are potential legal work arounds if Wyoming decides to not authenticate privately controlled public credentials.

1.2.3 Objectives:

Voir Dire's intent is to establish a decentralized Self Sovereign Digital ID (SSID) service, which enables the owner's control of specific semantic values and data that need to be authenticated by

---

‡ **NOTE:** The word “**ENTITY**” is used in various statutes (WS Titles 16, 17, 26, 28), typically referring to a Juridical PERSON, as opposed to a Natural PERSON. The proposed 26LSO-0012 refers (pg4, Ln 4, 9) to personal data protection policies, specifically referring to a Natural person, and then refers (pg6 Ln 7, 14) to a Wyoming Resident, regarding review and correction, while ignoring data collected that is required by law by a Registered Agent associating a Natural person with a Juridical person.

Wyoming for use in business registry, banking, smart contracts, transaction processing, and other activities. An effective SSID, reduces the dependency on current paper identification that releases collateral data that has been wholesale collected which 26LSO-0012 is meant to protect. While asserting specific facts (such as citizenship), other information can be withheld, protecting identities.

Employing Zero Knowledge Proofs to restrict data disclosure can facilitate the selective verification of LLC members or associates—potentially flagged by FinCEN as foreign or criminal actors—while mitigating risks from politically motivated phishing schemes or exposure in lawfare legal discovery.

1.2.4 Constraints:

This is not a formal specification which defines the robustness, or possible failures of cryptographic methods to protect personal data. At the time of this writing, Quantum processing is not a factor in protecting personal data collected by the government.

1.2.5 Assumptions:

The intent of developing a Self Sovereign ID is for lawful purposes to assert Semantic Information Elements of fact, endorsed or authenticated by issuers of credentials.

This document asserts the use of typical big-integer mathematics, prime numbers, and computations. Specific implementations may or may not be standardized.

Implementation of digital ledger technology(DLT) may or may not use blockchain algorithms, however, any DLT must provide functions (self stored) to access any public key, or internal encrypted or plaintext record.

1.3 Audience

The assumed audience is legislators, stakeholders, and software developers.

1.4 Definitions

For the purpose of this document:

A **semantic value** refers to the meaning or interpretation assigned to a word, phrase, symbol, or expression (the concept you relate to in your head).

A **semantic definition** means a definition structure consisting of descriptive attributes (name, assigned number, description, type, dependencies, and valuation / validator).

A **semantic dictionary** is a sorted set of semantic definitions, typically referred to as a schema.

An **Information Element** (IE) is a reference structure which cites the semantic dictionary, semantic assigned number, and a value object.

A **Digital ID** is a storage model of Information Elements for managing the digital identity of a unique

entity (natural or constructed) which includes specific attributes and credentials that are machine readable.

A **Self Sovereign ID** (SSI) is a Digital ID that reflects stored attributes and credentials that refer to external authorities (credential issuers) which can be proven to be issued by the authority, and held by the semantic entity who presents the Self Sovereign ID. The intent of a Self Sovereign ID is to be self issued rather than government issued identification. Nothing prevents an Entity from maintaining their own copy of the credential rather than referring to external issuer servers.

A **One-Way Function** is the process that is easy to convert inputs to an output, but impossible to determine the input from an output. Examples are digital signatures, password hashing, and public-key encryption. Also, an x-ray with an encrypted patient name in a stack of unlabeled millions is useless to determine whose record. But a patient with the record number and decryption key, can find it and prove it is theirs.

A **Verified Credential** is a digital or physical document that has been authenticated to confirm the identity, qualifications, or attributes of an individual or entity. It is typically issued by a trusted authority (government, institution, or organization) that contains verifiable data that can be checked against a reliable source to ensure its legitimacy. Credential verifiability includes digital signatures, multi-key encryption, or other methods that allow 3rd parties to confirm its authenticity and credential owner.

The **IPFS – Inter-Planetary File System** is a One-Way function peer-to-peer protocol which stores content by a hash file name rather than a location (such as a URL).

A **Zero Knowledge Proof** (ZKP) is a cryptographic method where a prover demonstrates to a verifier that a statement is true without revealing any additional information beyond the fact that the statement is true.

An **Immutable Ledger** is a record-keeping system, typically digital, where data is stored in a way that cannot be altered or deleted once entered. An example, although not limited to, is a blockchain.

2 Current Status

Unlike other states that have enacted broad consumer privacy laws, granting residents rights such as data access, deletion, and opt-out of the sale of data, Wyoming has yet to implement a comprehensive statewide framework governing the general handling of personal data by private entities.

In this age of lawfare and cancel culture, Wyoming's safest strategy is to encrypt everything and when ever possible disassociate identifiers and data (De-identified data), keeping each of this list separated: Name, Location, Phone numbers, SSNs, and pictures. As mentioned above, use One-Way functions (hash keys) and Zero Knowledge Proofs, rather than direct links or plaintext fields.

While it may seem obvious, it bears emphasizing that "De-identified data" (26LSO-0012, p. 2, ln. 7), whether stored off-chain or obscured among thousands of similar records, provides the essential abstraction to prevent actionable exposure ONLY if it achieves true anonymization rather than mere pseudonymization. Even then, such data must be regarded as personal and rigorously protected against re-identification, including when combined with supplementary information.

Transitioning state systems is inevitable to safeguard essential information, disclosing only the minimum required, while standardizing private data to eliminate redundancy and synchronization challenges. Ultimately, data's credibility is no stronger than its underlying proof; documents such as utility bills and leases are readily forged. This extends beyond Wyoming as a national challenge, concerning the private data mandated for government services and the dependence on potentially repudiable evidence to verify asserted facts.

Can private data be Repudiated?

REPUDIATION is the number one cause of Internet fraud, malware injections, voting fraud, and phishing, spoofing, and identity theft.

Non-repudiation ensures that a party in a transaction or communication cannot deny their involvement or the authenticity of their actions. It provides:

Proof of Action: Guarantees that you can prove you sent or received a message, signed a document, or completed a transaction, preventing others from falsely denying their participation.

Trust in Digital Interactions: Enhances security in online activities like e-commerce, contracts, or data sharing by ensuring all parties are accountable for their actions.

Legal Protection: Offers evidence in disputes, as cryptographic methods (e.g., digital signatures) link actions to specific individuals or entities, making it legally enforceable.

Data Integrity: Confirms that the message or transaction hasn’t been altered, ensuring reliability.

For example, if you sign a digital contract, non-repudiation ensures you can’t claim you didn’t sign it, and the other party can’t deny receiving it, protecting you in agreements or disputes. How much of personal data collected by the state, can be repudiated with no chain of proof?

Does Wyoming's LLC veil still provide privacy with FinCEN's Actions?

FinCEN's Corporate Transparency Act, the Bank Secrecy Act, and now the Real Estate Act (in effect Dec 2025), compels private data to be collected by 3rd parties who generally can not be held accountable in a malicious or accidental breach blaming FinCEN's requirements to collect it. Exposure-creep isn't limited to FinCEN demands, but also the State and Registered Agents. Just because Wyoming is not a reporting state, doesn't mean that the proxy who registers the entity is secure and immune from breach.

Because of the attractiveness of a Wyoming single-member LLC, whether seeking a trust's asset protection, or establishing an LLC for providing formal Business services or products, the entity (BOI) buying the registry must provide (BOI-Beneficial Ownership) information. Assuming that the BOI is not a Wyoming resident, and that banks in other states will assess risk differently for a business based in Wyoming, Out of State members require an authorized manager or registered agent to facilitate establishing a Wyoming financial account for proceeds and distributions, taking advantage of Wyoming's lack of income tax.

This opens another issue of non-BOI entities (acting with authority of a manager or the operating

agreement) directed to establish an account, which many banks and credit unions consider too risky if the principle is not present. The perception is that single-member Wyoming LLCs with an out-of-state member is a higher risk due to illegal activities hidden by Wyoming's privacy laws.

Note that Colorado law required a full C-Corporation business officer to secure a US Bank account under its corporate EIN, but using his personal credit score(800). When US Bank debanked that business, they also froze 7 lines of business and his personal credit and seized all business deposits, despite there being no incidents or derogatory information. Many Wyoming banks and credit unions refuse to allow the creation of business accounts unless the BOI is present.

The answer to this is for Wyoming to establish a dual-key entity database (blockchain) that enables a juridical or natural person to create a record that enables the person to prove control and ownership of the record. That record can be used as identification for proof of ownership of the registered business, and can be referred to a financial institution, and if requested by FinCEN, can be referenced.

Voir Dire's intent, is that the owner of this entity record needs verified credentials, including State agencies (DMV, Election, etc) and Notaries and under the 1866 Civil Rights Law, and the 14th Amendment, keeping birth records, proof of residency and US Citizenship assertions is State, not Federal responsibility.

The problem being solved is to verify an attribute defined by a Semantic Glossary, such as nationality based on ISO 3166-1 numeric code. If it is a public record, verified by the state or a notary, it is signed by authority's and owner's private keys. “Is the owner a US Citizen?” can be verified by ZKP to produce the field or answer the question. The issue is unless you have the owner identified, and have their corresponding public key (an open field in an SSID), there is no means of digital proof.

What about digital proof of other Wyoming assertions?

As Balcony is doing for New Jersey, putting deeds into a blockchain, A Wyoming effort would be welcomed to associate parcels with an OWNER-Entity, and legal residencies to a parcel, and a RESIDENT-Entity to a residency, and a keyed proof of ownership of the RESIDENT-Entity, has just solved the election integrity non-repudiated voter ID problem, including enabling secure voting over the Internet, and using blockchain tools, enabling independent Public audits and tabulation without scanners, all without exposing personal data.

By Wyoming not creating a formal immutable ledger of Entities, Wyoming is subjecting itself to speculation that Wyoming juridical persons are simply shell entities to obscure criminal activity, and that does not reassure Wyoming financial institutional fears when Agents attempt to establish Wyoming businesses accounts for entities they represent.

FinCEN's "Know Your Customer" requirements are eroding the protective abstraction of data. It is improbable that FinCEN will relent on its overreach or presumption of guilt for the innocent without data collection laws adopting a more GDPR-oriented framework. That protection is the benefit of using Zero Knowledge Proofs.

Creating a ZKP protected Entity record, does not prohibit current processes, but begins the inevitable transition to verified credentials, for Self-Sovereign Identification systems and increases reliability of State held data, while keeping data encrypted, reducing liability and exposure in the event of a breach.

Key concepts to keep in mind (based on GDPR prior art)

Data Minimization: Organizations must collect only the data strictly necessary for a specific purpose, Reducing the volume of sensitive data exposed to potential breaches.

Purpose Limitation: Data can only be processed for the specific, explicit purpose for which it was collected, and not reused for unrelated purposes without consent, limiting exposure to unauthorized entities.

Lawful Basis for Processing: Organizations must have a legal basis to process data, such as: consent, legal obligation, and contractual necessity or legitimate interest. Data is only exposed for regulatory purposes, not discretionary use.

Data Subject Rights: The right to control their data, including the right to access/review, the right to rectification, right to deletion when no longer needed, the right to restrict unassociated usage, and the right to data portability.

Data Security Requirements: Organizations must implement technical and organizational measures to protect data, such as encryption, pseudonymization, and access controls to secure against breaches.

Data Breach Notification: inform affected individuals.

Restrictions on Data Transfers: Restrict data sharing unless owner allows, and recipient ensures equivalent protections.

Accountability and Governance: Organizations must maintain Data Protection Officers responsible for developing and enforcing policies for data collection, access, security, privacy, and usage across executive branch agencies.

Isn't REAL-ID enough?

Wyoming's Public Records Act and European Union's GDPR are two actions intended to set strict rules of how select personal data is protected. Since May 2025, The 2005 Real-ID Act - a hybrid Federal/State quasi National ID that is built on State issued driver's licenses, is now in full enforcement. Real-ID provides by simple photocopy, exposure of non-selective information to non-federal institutions.

Through REAL-ID, bulk personal data is collected and distributed, yet in 2020, U.S. Customs and Border Protection seized 19,888 counterfeit U.S. driver’s licenses at Chicago O’Hare International Airport, mostly from China and Hong Kong, intended primarily for college-age students. A 2025 FBI report, declassified by Director Kash Patel, alleged Chinese involvement in producing fake licenses for a 2020 election interference scheme via mail-in ballots, meaning REAL-ID is ineffective.

The issue facing “verifiable” identification is known as **repudiation**, which, based on the legal term, enables the denial of authority such as a signature on a contract. Fraud depends on the inability to absolutely verify factual identity allowing click bait phishing, phone scams, and other “unverified” credential crime including filing false records to government agencies.

The solution to this is the adoption of non-repudiated credentials that require specific secret

information known only to the presenter of identification. But solving repudiation is only part of the current problem. **Bulk data collection is shared without requiring proof of necessity.**

As mentioned above, the Civil Rights act of 1866 and the 14th amendment, states are responsible to preserve birth records, establish residency and US Citizenship. To my knowledge, no state provides the necessary infrastructure for non-repudiated digital identification by creating an immutable record of birth which is digitally signed by the natural person it is for. No state currently uses an immutable ledger such as blockchain to maintain authority over parcels of land and their subdivision or transfer. No state establishes an immutable record of legal residences, where ownership of a parcel is the verifier of who claims to be resident.

Implementing these digital credentials, signed by the owner, would greatly enhance security of the stored data, and enable non-repudiated identity for smart contract transactions. This would eliminate fraudulent property titles and theft, enable residency claims for an off-grid property that doesn't receive utility bills, and other advantages.

Voir Dire's SSI solution is justifiable for proof of ownership, authentication, smart contracts, and financial accounts for transaction processing, but it is missing state endorsements and interfaces that would eliminate fraud, provide non-repudiated voter Identification, verify residency, and citizenship, whether Wyoming participated or not.

What is the purpose of Voir Dire llc?

“Voir dire”, meaning "to speak the truth," is a legal process used to question prospective jurors or witnesses to ensure their suitability and reliability. The same applies to assertions of digital rights claims. While “voir dire” itself is about questioning people, it indirectly supports verifying truthful content by vetting challenges following the Chain Of Proof versus claims which can be repudiated.

Voir Dire, llc's has a number of decentralized roles to enable a user to create a Self Sovereign Identity, store data references (DIDs), create IPFS-like references, establish digital wallets and public / private keys. Users can place in their SSID, medical records, financial accounts, skill credentials, and other digital data that should not be under control of unaccountable 3rd party platforms. Instead the SSID can be downloaded or stored in redundant decentralized storage locations, and not on the platform itself.

Voir Dire, llc, is a decentralized processing scheduler, utilizing decentralized managed data storage, to perform Zero Knowledge Proofs and access credentials which are stored in the decentralized cloud, initiated by the user,

Voir Dire is developing online services as well as a digital card, and two other devices, that can be used to provide Point of Sale merchant services as well as identification, proof of credentials, and other forms of digital verification.

Voir Dire's proposed Self-Sovereign ID, utilizes a semantic dictionary used to validate, store, and properly form individual facts, critical to Zero Knowledge Proofs. Built on numerous definitions from commonly accepted sources such as Schema.org.

Voir Dire's escrow service maintains many kinds of references between public references and public keys, such as email to key records. Services will begin in late 2025.

SUMMARY

Wyoming’s approach reflects its libertarian-leaning culture, which values individual privacy and limited government interference while recognizing the need for public accountability in a sparsely populated state where government plays a significant role.

FinCEN implicitly recognizes the financial independence of Wyoming LLCs by treating them as separate legal entities under the BSA, CDD Rule, and other regulations. This is consistent with Wyoming’s LLC Act, which establishes LLCs as distinct from their members (W.S. § 17-29-104). However, FinCEN imposes uniform compliance requirements (e.g., CTRs, SARs, and previously BOI reporting) with no exemptions for claims of "independence." The 2025 BOI exemption for U.S. LLCs simplifies reporting but does not alter their status as independent entities for financial regulation.

In the current vacuum of digital identification, legislation that enables credentials that can be repudiated, or merely allows an image on a digital device, doesn't solve the problem of government overreach of collected data, nor does it prevent non-government institutions from acquiring personal data.

The Federal Privacy Act (5 U.S.C. § 552a) limits disclosure of personal records without consent but explicitly allows release if FOIA requires it (i.e., no exemption applies). For state-submitted data, if it's not "personally identifiable" or if public interest outweighs privacy (e.g., via a balancing test), it can be disclosed. Agencies must notify submitters of potential release for certain data (e.g., trade secrets).

What can the subject of private data do to protect themselves from wholesale release or malicious intent? Voir Dire's position is for the state to request permission to the exposure of private data, and to implement State structures that utilize digital methods that can be chained.

Action Items

The primary task is to provide digital identification for smart contracts. For the State, it is to ensure person data to service the census, justify representation, enable non-repudiated voter id with chain of proof, obtain services from the state, and establish the obligation of the state to verify credentials of a digital person record.

To enable this, Wyoming should establish a semantic glossary for person data fields (based on a sources such as Schema.org), Broaden the legal PERSON definition to include a juridical (legal constructed) person. Establish a blockchain for Self registered persons. Establish Electronic Notarization System for submission of documents, proof of control, and verification of association and meeting Semantic definition. Ex: verify state of birth and US citizenship from a passport as a verifiable credential. Extend all Wyoming records, to ownership by Person ledger which contains person's self protected data. Ensure that Registered Agents are held to protection of business data as agents of the state. Require the BOI Person Record signature for Business filings. Require person record allowance grant by owner for bank account establishment. And as Balcony is doing, Create chain of proof for: Subdivided parcels, Parcel to owner relations, creating a legal Residence Database, relating Residence to Parcel, and if the person record includes the linkage of residence and resident with owner's signatures, have a verifiable voter ID.