Policy	Category	Relevance to Identity Systems	Implications for Identity System Users
EU GDPR - **G**eneral **D**ata **P**rotection **R**egulation [41]	Legislation	Not directly mention, but key principles, such as minimizing data collection (Article 5. data minimization) and giving users rights over their data (Article 12. transparency, Article 20. right to data portability), forms how identity systems store and process personal data.	GDPR emphasizes user control over personal data, granting individuals rights to access, correct, delete, and port their identity data. For users of identity systems, this means they should be able to manage their data actively and transparently. Moreover, GDPR's data minimization principle encourages identity systems to verify users with the least amount of personal information necessary.
eIDAS - **e**lectronic **ID**entification, **A**uthentication and trust **S**ervices 2.0 [21]	Legislation	eIDAS 2.0 amends the original eIDAS Regulation on electronic identification and trust services to reflect the growing need for secure and accessible digital identity across the EU. It introduces the EU Digital Identity Wallet, enabling all EU citizens, residents, and businesses to securely verify their identity and present required personal attributes when accessing both public and private services.	Users can access services like banking, university applications, or age verification using a single EU Digital Identity Wallet on their phone. Instead of showing full IDs, they can share only necessary attributes (e.g. age 18+). The wallet works across all EU countries, supports both public and private services, and includes features like a privacy dashboard and free eSignatures. Users stay in control of what data they share and with whom.
U.S. BSA - **B**ank **S**ecrecy **A**ct [22]	Legislation	The BSA is the U.S. anti-money laundering law. It requires financial institutions to verify the identity of customers opening accounts and maintain records of the information used to verify identity (31 U.S.C. 5318).	Users will be asked for personal identification (like ID documents or Social Security number) whenever you engage with regulated financial services. Still, BSA compliance often creates privacy risks due to the large amounts of personal data stored by banks.
CCPA - **C**alifornia **C**onsumer **P**rivacy **A**ct [9]	State-level Law	Not directly mention, but regulate businesses' handling of personal information (1798.100 - General Duties of Businesses that Collect Personal Information, 1798.105 - Consumers' Right to Delete Personal Information, 1798.110 - Consumers' Right to Know What Personal Information is Being Collected. Right to Access Personal Information etc.)	Users can recieve clear explanations of what personal information is being collected and for what purpose. They also have the ability to access or delete their data, with appropriate identity verification required to protect their privacy.
CPRA - **C**alifornia **P**rivacy **R**ights **A**ct [43]	State-level Law	Not directly mention, but CRPA strengthens and expands CCPA's protections (1798.121), particularly for sensitive identity data. It adds a new category of "sensitive personal information", such as government ID numbers, biometric data, that gets extra safeguards.	Users gain the enhanced right to limit the use and disclosure of their sensitive personal information by businesses.
California State Law [10]	State-level Law	California authorizes county recorders to issue birth, death, and marriage certificates using blockchain-based verifiable credentials (SB786).	Users have greater control over their identity documents and benefit from reduced reliance on paper copies as technical safeguards to prevent fraud and unauthorized or illegal access, destruction, use, modification, and disclosure.
Arizona State Law [24]	State-level Law	Arizona amended its Electronic Transactions Act to recognize signatures and records secured via blockchain as legal electronic signatures and records (HB 2417). This provides legal validity to smart contracts and potentially to blockchain-based credentials, laying groundwork for DIDs.	Users can use blockchain-based IDs and contracts with legal legitimacy.
Wyoming State Law [2]	State-level Law	Wyoming legally defined "personal digital identity" as an intangible digital representation of a person (§ 40-30-101). It clarifies that actions through a digital identity are attributable to the person.	Wyoming reduces legal ambiguity for users controlling their identity data, and it provides users legal recognition of digital identity actions.
Utah State Law [25], [42]	State-level Law	Utah enacted a law to launch a pilot for blockchain-based digital verifiable credentials (HB 0470). It requires consulting privacy officers on how to safeguard personal data in the system. Utah also passed the digital identity act outlining principles for state-endorsed digital IDs (SB0260), emphasizing user control, privacy protections, selective disclosure, and voluntary participations.	Users can rely on legal protections that prevent their digital identity from being surveillanced, tracked, or monitored. The state guarantees that any use remains limited to the original purpose, and that individuals can disclose only the specific identity attributes needed.
NIST SP 800-63 Digital Identity Guidelines [31]	Standards, Requirements	NIST Special Publication 800-63 is a set of guidelines for digital identity, divided into 63-3/63-A/63-B/63-C. SP 863-3 provides the overarching framework, introducing key concepts and assigning levels of assurance based on the rigor of the process. SP 800-63A focuses on the process of verifying an individual's identity, outlining technical requirements for different methods (e.g., in-person, remote). SP 800-63B addresses authentication, detailing requirements for authenticators (such as passwords, biometrics, or tokens). SP 800-63C provides guidance on federation.	If an online service follows NIST guidelines, it can tailor the level of identity proofing and authentication based on the risk associated with the service. For low-risk scenarios, minimal identity checks and simpler login methods (e.g., passwords) may be sufficient. For high-risk services, like accessing sensitive personal records, more rigorous ID verification and stronger login protections (e.g., multi-factor authentication) are required. This risk-based approach allows organizations to achieve a balance between security and user convenience.
W3C Recommendation [15], [47]	Standards, Requirements	W3C is establishing and advancing technical standards for user-driven digital identity systems, such as DIDs, the Verifiable Credentials Data Model, and Controlled Identifiers. These standards define mechanisms that leverage decentralized technologies like blockchain to allow individuals to manage and present their own identifiers and credentials. The aim is to enable self-sovereign identity that ensures both privacy protection and interoperability.	W3C's identity standards mean greater control and flexibility over how they manage and share their personal information. Instead of relying on centralized platforms to issue and store their identities, individuals can create and manage their own identifiers and credentials, such as diplomas or IDs, on blockchain-based systems.
DHS Technical Implementation Requirements for Decentralized Identity [16], [17]	Standards, Requirements	DHS Silicon Valley Innovation Program released technical implementation requirements for decentralized identity systems. Users retain full control over their digital credentials, which can be selectively disclosed without exposing unnecessary personal data. The system avoids centralized tracking by eliminating back-channel communication and relies on open standards like W3C Verifiable Credentials and DIDs.	Instead of presenting full ID documents, they can use a mobile wallet to share only what's needed. There's no background data tracking when credentials are used, so users avoid unwanted surveillance.
FinCEN Guidelines [22]	Guidance, Recommendation	FinCEN is the U.S. agency that enforces BSA and oversees AML/KYC compliance. It issues guidelines and rulings that shape how institutions can use digital identity. Recent initiatives include: guidance that cryptocurrency exchanges are money service businesses thus must do KYC (FIN-2013-G001), FAQs permitting banks to use "non-documentary verification" like digital credentials.	The guidelines imply that users may see more modern identity verification using a trusted digital ID or biometric check instead of a photo of your driver's license when you open bank accounts. As FinCEN refines its guidance, it could become easier and safer to prove identity remotely, with banks able to rely on secure digital IDs that meet regulatory standards.
FATF Digital ID Guidance [23]	Guidance, Recommendation	FATF Digital Identity Guidance explains how digital ID systems can be used for identity verification under global AML/CFT regulations. It aligns international assurance frameworks such as NIST and eIDAS to assess reliability, and includes recommendations for governments and stakeholders on how to achieve trustworthy digital ID systems.	When these systems meet recognized assurance standards (e.g., NIST or eIDAS), users may benefit from faster onboarding and improved access to financial services. This supports financial inclusion, especially for those lacking traditional ID. However, users must also be aware of cybersecurity risks unique to digital ID, such as identity theft over the internet.
FTC Competition and Consumer Protection Guidance [13]	Guidance, Recommendation	The FTC Act is not a law specific to identity, but enforces several key guidelines that impact identity systems and identity verification. The Red Flags Rule requires certain financial institutions and creditors to detect and respond to signs of identity theft. The Safeguards Rule mandates that covered businesses implement security programs to protect consumer data, including measures like encryption and multi-factor authentication. The Identity Theft Report, available through IdentityTheft.gov, supports victims in reporting and recovering from identity fraud.	Users can expect service providers to monitor for unusual account access or use of fake credentials, as required under the Red Flags Rule. Personal information like names, Social Security numbers, or login credentials should be protected through safeguards such as encryption and multi-factor authentication under the Safeguards Rule. If identity theft occurs, users have the right to file an official Identity Theft Report through IdentityTheft.gov, which can be used to dispute unauthorized accounts, and obtain records from businesses involved.
OECD Recommendation of The Council on the Governance of Digital Identity [40]	Guidance, Recommendation	The OECD, an international organization that promotes global economic development and supports both advanced and developing economies, issued its Recommendation on the Governance of Digital Identity. It urges member states to build digital ID systems that are user-centered, privacy-preserving, secure, and accessible to all, including vulnerable groups. The recommendation promotes cross-border interoperability and consent-based systems that give users control over their personal data.	Without fast internet or digital skills, systems should be accessible via mobile or offline channels, with support available. If users lose access or face errors, clear recovery processes and help must be in place. Vulnerable users, such as migrants or people with disabilities, should be included through design features like multilingual support or alternative verification methods. Users shouldn't be restricted services if they choose not to use a digital ID.
EBSI - **E**uropean **B**lockchain **S**ervices **I**nfrastructure [26]	Strategic Framework	EBSI is EU's blockchain infrastructure for cross-border public services, developed as an initiative of the European Commission and the European Digital Infrastructure Consortium. EBSI enables the issuance and verification of credentials (e.g., diplomas, IDs) across member states. It aligns with the EU's eIDAS framework and aims to enable decentralized identity credentials used throughout the EU.	Users can use EBSI to share trusted credentials as proof of identity without needing to send paper documents or expose unnecessary personal details. For example, instead of uploading a full ID, they can prove just their eligibility for a service (such as being over a certain age). These credentials can be instantly verified across EU countries, making cross-border services more efficient and trustworthy.
NSTIC - **N**ational **S**trategy for **T**rusted **I**dentities in **C**yberspace [34]	Strategic Framework	NSTIC is a U.S. government-led strategy outlining a vision for building a secure and privacy-respecting digital identity ecosystem. The strategy promotes four key principles: privacy-enhancing and voluntary, secure and resilient, interoperable, and cost-effective and easy to use. It defines distinct roles: the private sector leads development, the government supports with coordination and standards.	Users no longer need to manage dozens of passwords across different sites. Instead, they can use a small number of trusted digital credentials that can be reused across services. Rather than repeatedly entering full personal details, users can share only the minimum necessary information. Participation is voluntary, and users can opt out at any time.