Principles and Progress in Digital Identity Systems - An Exploration of 12 Modern Identity Laws for Data Protection and User Sovereignty

Shahan Karim
DeID Tech Group
www.DeID.Tech
contact@shahankarim.com

***Abstract*—As the digital ecosystem continues to evolve, identity management is emerging as a critical focus area. The concept of identity has evolved significantly, transcending the traditional confines of physical documents to encompass a myriad of digital attributes. With this advancement, personal information has become a valuable commodity. The collection, storage, and use of personal information by organizations and governments has raised concerns about privacy and security, particularly considering increasing data breaches and identity theft while current methods often compromise user rights and security.**

This whitepaper, titled "Principles and Progress in Digital Identity Systems - An Exploration of the 12 Modern Laws for Data Protection and User Sovereignty," aims to delve into the complexities of digital identity systems, while elucidating a framework of principles that are needed to govern the current state and any progress made in this domain.

I. The Importance of Digital Identity in the Modern World

Digital identity has become an integral part of our lives. It serves as the digital representation of an individual's identity, encapsulating a range of data attributes, from basic personal information to intricate digital footprints. In the modern world, digital identity is not merely a convenience but a necessity. It underpins many activities, from online transactions and digital banking to immigration and medical records. It is the cornerstone of trust in the digital world, enabling secure and seamless interactions across digital platforms.

However, the importance of digital identity extends beyond individual convenience. At an organizational level, it facilitates customer onboarding, ensures secure transactions, and aids in regulatory compliance. At a societal level, it can promote inclusivity, enabling access to digital services for those traditionally excluded from the physical system due to geographical or socio-economic constraints.

A. The Problem with Centralized Identity Systems

Despite the undeniable importance of digital identity, the current systems are fraught with challenges, primarily due to their centralized nature. Centralized identity systems, where a single authority controls and manages identity data, have proven to pose significant risks.

Firstly, they present a single point of failure. In the event of a data breach, the consequences can be catastrophic, leading to the exposure of sensitive personal information on a large scale. The increasing frequency and sophistication of cyber-attacks exacerbate this vulnerability. For instance, identity fraud resulting from fraud losses hit $23 billion in total annual cost in 2022 [1], underscoring the severity of the threat.

Secondly, centralized systems often lack transparency and give users little control over their data. Users are usually unaware of how their data is being used or who has access to it. This lack of control and transparency can lead to misuse of data and infringement of privacy.

Thirdly, centralized systems can lead to inefficiencies and inaccuracies. The process of verifying and updating identity data can be time-consuming and prone to errors. Moreover, these systems often struggle to keep up with the dynamic nature of personal data, leading to outdated or incorrect information.

And fourthly, centralized systems hinder interoperability and maneuverability. We see this in systems that handle personally identifiable information or PII such as healthcare or driver licenses where one office or state is unable to utilize another office’s information that pertains to the user, partially owned by the user.

Identity is used to establish who we are, what we do, and what we stand for. However, the traditional centralized approach to identity management, procurement, life cycle, and attestation has proven inadequate and resulted in many challenges, especially in areas related to privacy, security, and control.

B. The Journey of Identity Procurement and Attestation

Traditionally, identity procurement has been a physical process. Individuals would obtain various forms of identification, such as birth certificates, passports, and driver's licenses, from trusted authorities. These documents would then

serve as proof of identity in various contexts, from opening a bank account to traveling internationally. However, this process over time has proven to contain significant risks, challenges, and limitations. Physical documents can be lost, stolen, or forged, and verifying their authenticity can be challenging and time-consuming.

The shift to digital identity systems represents a significant advancement in identity procurement. Digital identities are not only more convenient for users, but they also offer enhanced security features, such as biometric data and cryptographic keys, making them harder to forge. Furthermore, digital identities can be verified instantly, making the process more efficient for both users and service providers.

C. Shift to Digital Identity Systems

With the advent of the digital age, the process of identity procurement has shifted online. Digital identity systems leverage technology to streamline the procurement process, making it more efficient and user-friendly. These systems typically involve the creation of a digital identity profile, which contains a range of personal data attributes. The procurement process may involve various forms of online verification, such as email confirmation, biometric checks, or multi-factor authentication.

However, the shift to digital has also introduced new challenges. The online environment has opened new avenues for identity theft and fraud. Moreover, the proliferation of digital platforms has led to the fragmentation of digital identities, with individuals often having multiple, disjoint identities across different platforms. This fragmentation can lead to inconsistencies and inaccuracies, undermining the reliability of digital identities.

D. The Role of Attestations in Identity Verification

Attestations play a crucial role in the identity verification process. An attestation is confirmation by a trusted entity that a certain claim about an individual's identity is true. In the context of digital identity, attestations can take various forms, such as a digital signature from a trusted authority confirming the validity of a document, or a verification code sent to a user's phone to confirm their possession of the number.

Attestations add a layer of trust to the digital identity system, providing assurance that the identity data is accurate and reliable. However, they also introduce new complexities. The process of issuing and verifying attestations needs to be secure and robust to prevent fraud. Moreover, in identity systems, the question of who can issue attestations and how they are trusted becomes critical.

E. Current Challenges with Digital Identity Systems

Technological advancements have had a profound impact on identity systems. On the one hand, they have enabled more efficient and user-friendly identity verification processes, facilitated the integration of biometric data into digital identities, and opened new possibilities for decentralization. On the other hand, they have also introduced new vulnerabilities and complexities. The increasing use of AI and machine learning in identity verification, for instance, raises questions about privacy and bias. The proliferation of IoT devices expands the scope of digital identities but also increases the risk of data breaches.

Some key problems currently plaguing the digital identity landscape include:

1) Cost of Data Breaches:

Identity fraud losses totaled $52B in 2021, affecting 42 million U.S. adults. 1 in 20 Americans were victims of fraud in 2021 [2]. Losses from identity theft are predicted to grow to $635.4 billion by 2023 [3]

2) Lack of User Data Sovereignty and Privacy:

Existing systems often fail to place control of digital identities in the hands of the users themselves. Users frequently have no say over who has access to their personal information and how it is used, violating their right to privacy. Eight-in-ten Americans say they have very little or no control over the data collected about them by the government (84%) or by companies (81%) [4].

3) Security Concerns and Data Breaches:

Traditional, centralized digital identity systems represent a significant security risk. These single points of failure can, when compromised, expose vast amounts of sensitive user data. Eighty-three percent of organizations studied have experienced more than one data breach, and just 17% said this was their first data breach [5].

4) Lack of Interoperability and Standardization:

Many digital identity systems operate in isolation, leading to fragmentation and inefficiencies. Users are often required to maintain multiple digital identities across different platforms, increasing complexity and the risk of security breaches.

5) Inadequate User Experience (UX):

Complex registration processes, forgettable passwords, and other UX challenges can make digital identity systems difficult to use. Poor UX design can result in low system adoption and user dissatisfaction.

These challenges underscore the need for a novel approach to digital identity - one that prioritizes data sovereignty and privacy, addresses security concerns, promotes interoperability and standardization, and focuses on improving user experience.

F. The Need for an Updated Framework to Address Current Challenges

In light of these concerns, there is a pressing need for an updated framework that can guide the development and governance of digital identity systems. This framework or known in this paper as laws should reflect the realities of the modern digital landscape, addressing the challenges posed by technological advancements and evolving societal norms. They should promote privacy, security, transparency, and user sovereignty, while also accommodating the potential of emerging technologies such as decentralization.

This process of understanding and analysis has brought us to using a few select naming conventions. We chose to use the word “Laws” to denote a scientific approach to understanding

the origins of our hypothesis and to provide a framework built from testable observations and concepts that allow for a genuine discourse. As the intent is along scientific lines, we are not proposing to enter in a discussion about Identity Philosophy nor create any misunderstandings of legal or moral edicts.

As we navigate the complexities of the digital age, the need for a robust and comprehensive framework to govern digital identity systems becomes increasingly apparent. The evolution of Kim Cameron's Laws of Identity, which were instrumental in shaping the initial stages of digital identity, has paved the way for a new set of principles that reflect the current digital landscape. These modern identity laws aim to address the challenges posed by technological advancements and the evolving nature of digital interactions.

The following section will introduce the proposed modern identity laws, providing a detailed exploration of each law and its relevance in the current digital identity landscape.

II. Law 1: The Law of Self-Sovereign Identity: Individual Sovereignty

The first law in our modern identity framework is the Law of Self-Sovereign Identity. This law posits that individuals should have complete control over their digital identities. It shifts the ownership of identity from centralized authorities to the individuals themselves.

A. Understanding Self-Sovereign Identity

Self-sovereign identity (SSI) is a concept that empowers individuals with the autonomy to manage their digital identities. Under this model, individuals can create their digital identities, manage their personal data, and control how, when, and to whom their identity information is disclosed. This approach contrasts with traditional identity systems, where a central authority or third-party organization holds and controls individuals' identity data. It aims to tackle the problem of identity fragmentation, where individuals have multiple identities across different platforms and services. This also addresses another challenge, interoperability, and integration, allowing the information to be moved between systems freely and verifiably in a secure manner.

For self-sovereignty to occur, individuals must be involved in the process of using verifiable credentials. With ownership shifted, users will be required to provide consent to use those credentials or identifiers. We must understand that individuals may be broadened to include organizations, pseudonymous identities, and governments.

B. Implications of the Law of Self-Sovereign Identity

The Law of Self-Sovereign Identity promotes user empowerment and inclusivity. By giving individuals control over their identities, it allows them to participate fully in the digital economy, irrespective of their geographical location or socio-economic status. It also enables individuals to assert their identity in a digital context without relying on a central authority, which can be particularly beneficial in regions where access to official identity documents is limited, controlled, or lost. Some additional areas of implication include:

1) Privacy Protection

By giving individuals control over their digital identities, this will aid in helping to protect user privacy. Users can decide what personal data to share, with whom, and for what purpose, thereby maintaining control over their personal information.

2) Trust and Verification

The Law of Self-Sovereign Identity can enhance trust in digital interactions. When individuals have control over their digital identities, they can verify their identity to others in a secure and reliable manner, enhancing trust in online transactions further increasing participation and inclusion

3) Inclusion

Self-Sovereign Identity can promote social and economic inclusion. By providing a secure and reliable means of proving one's identity, self-sovereign identity systems can enable access to essential services such as banking, healthcare, and education, particularly for marginalized or underserved communities.

For example, a use case of self-sovereign identity is in the healthcare industry, where individuals have control over their medical information, including the ability to choose what information is shared with healthcare providers and other organizations. This helps to ensure that medical information is protected from unauthorized access and misuse, and that individuals have control over their own health information. Additionally, allows the ease of sharing medical information between care providers or emergency situations where verifiable information is vital to assist in someone's survival.

C. Challenges and Considerations

Verifying the authenticity of self-sovereign identities can be complex. Without a central authority to vouch for the accuracy of identity data, new mechanisms for trust need to be established. Artificial Intelligence and Distributed Ledger technology, with its adapted and decentralized immutable nature, offers a potential solution to this challenge.

Furthermore, the implementation of self-sovereign identity requires careful consideration of user experience. While control over identity data is crucial, it should not come at the expense of usability. Designing intuitive interfaces and processes that allow individuals to manage their identities effectively is a critical aspect of implementing this law, especially for accessibility.

The Law of Self-Sovereign Identity sets the foundation for a user-centric approach to digital identity, promoting privacy, security, and user empowerment. Some areas to consider:

1) Technical Complexity

Building a self-sovereign identity system can be technically complex. It requires advanced technologies, such as distributed ledgers and advanced cryptography, to ensure that identities are secure, verifiable, and under the control of the individual.

2) User Education

Many users are not familiar with the concept of self-sovereign identity. Educating users about their rights and responsibilities under a self-sovereign identity system is a significant challenge.

3) Interoperability

For a self-sovereign identity to be useful, it must be recognized and accepted by various entities, including businesses, governments, and other organizations. Ensuring interoperability between different systems and entities is a major challenge.

4) Legal and Regulatory Compliance

Self-sovereign identity systems must comply with a range of legal and regulatory requirements, including data protection and privacy laws. Navigating these requirements can be complex, especially for global systems that operate across multiple jurisdictions.

5) Security

While self-sovereign identity systems can enhance security by decentralizing data, they also present new security challenges. For example, if an individual loses their private key, they could lose access to their digital identity. Ensuring the security of self-sovereign identity systems is a significant challenge.

6) Adoption

For self-sovereign identity systems to be successful, they must be widely adopted by both users and entities. Encouraging adoption can be a challenge, particularly given the technical complexity and unfamiliarity of self-sovereign identity.

III. Law 2: The Law of Decentralization

The second law in our modern identity framework is the Law of Decentralization. This law asserts that digital identity systems should be decentralized, distributing control and authority, and enabling a peer-to-peer network of communication. Systems should leverage Decentralized Credentials and Identifiers that remove the need for and use of a central authority.

A. Understanding Decentralization

The Law of Decentralization advocates for the distribution of control over identity data among multiple parties, rather than concentrating it in a single central authority.

In a decentralized identity system, an individual's identity data is not stored in a central database. Instead, the control of identity data is distributed among the users themselves and possibly other decentralized entities. This approach enhances privacy, as users have more control over their personal data and who has access to it. It also increases security, as there is no single point of failure that could lead to a large-scale data breach.

In essence, the Law of Decentralization is about shifting control over identity data from centralized authorities to the individuals themselves, thereby enhancing privacy, security, and data sovereignty for users.

B. Implications of the Law of Decentralization

The Law of Decentralization has significant implications for privacy, security, resilience, and innovation in digital identity systems. Some additional areas include:

1) Privacy Enhancement

Decentralization can enhance privacy by reducing the amount of personal data held by any single entity. This can reduce the risk of large-scale data breaches and misuse of data.

2) Increased Security

Decentralized systems can be more secure than centralized ones because they distribute risk. If one part of the system is compromised, the damage can be contained and does not necessarily affect the entire system.

3) Resilience

Decentralized systems can be more resilient than centralized ones. Because they do not have a single point of failure, they can continue to function even if part of the system fails or is attacked.

4) Promotion of Innovation

Decentralization can promote innovation by allowing for a diversity of approaches and solutions. This can lead to the development of new and improved digital identity services and applications.

By adhering to this law, digital identity systems can enhance privacy and security, empower users, increase resilience, and promote innovation.

C. Challenges and Considerations

While the Law of Decentralization offers many benefits, it also presents new challenges. Designing and implementing a decentralized identity system can be complex, requiring careful coordination between the different entities involved. Ensuring the security and privacy of the system is also more challenging in a decentralized context, as the distributed nature of the system creates multiple potential points of attack. Some areas of consideration:

1) Technical Complexity

Decentralized systems can be technically complex to design and implement. They require sophisticated protocols and algorithms to ensure that all parts of the system can communicate and coordinate effectively.

2) Security Risks

While decentralization can enhance security by distributing risk, it also introduces new security challenges. For example, ensuring the integrity and authenticity of data in a decentralized system can be challenging.

3) Governance

Decentralized systems require effective governance mechanisms to coordinate the actions of the various parties involved and to resolve disputes. Designing and implementing these governance mechanisms can be a complex task.

4) User Experience

While decentralization can enhance user sovereignty, it can also make systems more difficult to use. For example, users may need to manage their own keys in a decentralized identity system, which can be a challenging task for non-technical users.

5) Legal

Decentralized systems can pose legal challenges. For example, it can be difficult to assign responsibility for data breaches or other issues in a decentralized system.

Furthermore, the Law of Decentralization raises questions about governance. In the absence of a central authority, new mechanisms are needed to establish trust, resolve disputes, and coordinate updates to the system. Systems that leverage consensus mechanisms and smart agreements offer potential solutions to these governance challenges.

IV. Law 3: The Law of Privacy

The third law in our modern identity framework is the Law of Privacy. This law emphasizes that personal attributes or information contained within our digital identities must be protected and stored in a confidential matter where applicable. This law is necessary to address the problems associated with centralized identity systems, which often lack privacy protections and result in the exposure of sensitive personal information.

A. Understanding Privacy

Privacy in the context of digital identity refers to the right of individuals to have their information protected in a confidential manner in order to limit exposure. Our privacy is usually defined in the digital realm as PII and it is here where we feel user control and confidentiality is paramount. Protection from improper use, disclosure, and the allowance of obscurity is a primary requirement for digital identity systems.

Additionally, this concept addresses the need for systems to consider pseudonymity and circumstances such as witness protection where a usable identity must be generated and still have connection in a protected fashion to an original representation of a digital identifier.

B. Implications of the Law of Privacy

Digital identity systems must implement robust data protection measures to ensure the privacy of personal information. This includes using strong encryption methods to secure data both at rest and in transit, as well as implementing strong access controls to ensure that only authorized individuals can access personal data. Some areas include:

1) Data Protection

Digital identity systems must implement robust data protection measures to ensure the privacy of personal information. This includes using strong encryption methods to secure data both at rest and in transit, as well as implementing strong access controls to ensure that only authorized individuals can access personal data.

2) Consent:

In line with the Law of Privacy, digital identity systems must obtain user consent before collecting, using, or sharing personal data. This ensures that users have a say in how their data is used and helps to build trust in the system.

3) Transparency

To uphold the Law of Privacy, digital identity systems must be transparent about how they collect, use, and protect personal data. This includes providing clear and accessible privacy policies and notifications.

4) Compliance

Many privacy laws and regulations, such as the General Data Protection Regulation (GDPR) in the EU and the California Consumer Privacy Act (CCPA) in the US, require businesses to protect personal data and uphold user privacy. By adhering to the Law of Privacy, digital identity systems can help businesses comply with these and other regulations.

5) Trust

Upholding privacy is crucial for building user trust. When users trust that their personal data will be kept private and secure, they are more likely to use and engage with the digital identity system.

C. Challenges and Considerations

While the Law of Privacy offers significant benefits, it also presents challenges. Ensuring privacy in a digital context can be complex, due to the vast amounts of data generated by online activities and the ease with which this data can be collected, stored, and shared. Implementing privacy-enhancing features can also be technically challenging and may impact the usability of the system. Some areas of consideration:

1) Balancing Privacy and Functionality:

While privacy is crucial, it must be balanced with the functionality of the digital identity system. Too many privacy controls can make the system cumbersome to use, while too few can compromise privacy. Striking the right balance is a significant challenge.

2) Data Minimization

The principle of data minimization — collecting only the data that is necessary — is a key aspect of privacy. However, determining what data is "necessary" can be a complex task, especially given the diverse range of services and functionalities that digital identity systems can provide.

3) User Education

Many users are not fully aware of the importance of privacy or how to protect their privacy online. Educating users about privacy and how the digital identity system protects their privacy is a significant challenge.

4) Technological Advances

Technological advances, such as the rise of artificial intelligence and machine learning, present both opportunities and challenges for privacy. These technologies can enhance privacy protections but can also be used to infringe on privacy if not used responsibly.

5) Privacy by Design

Implementing privacy by design — integrating privacy protections into the design of the digital identity system from the outset — is a best practice but can be challenging to implement in practice.

V. Law 4: The Law of Security

The fourth law is the Law of Security. This law states that digital identities and the systems they utilize or generate them

must be designed in a ground up manner to be secure and protected from unauthorized access or tampering.

A. Understanding Security

In the context of digital identity, security refers to the measures taken to protect personal data from unauthorized access, use, disclosure, disruption, modification, or destruction. This includes a wide range of measures, from encryption and access controls to intrusion detection systems and secure software development practices.

Advancements in security challenges have drastically changed how we understand user interaction and activity in systems. Tactics leveraging phishing, social engineering, and physical intrusion have become ubiquitous. To solve this, multiple layers of security have proved to provide the best path of defense. By leveraging advance systems, processes and technologies such as Implementation of deep neural networks, Artificial Intelligence, zero-knowledge proofs, biometric identifiers, and quantum cryptography will aide in providing additional solutions for addressing these critical areas as we progress in our system design and secure development practices.

B. Implications of the Law of Security

The Law of Security, which states that digital identity systems must always ensure the security of personal data, has several significant implications:

1) Robust Security Measures

Digital identity systems must implement robust security measures to protect personal data. This includes strong encryption methods, secure user authentication mechanisms, and advanced threat detection and response capabilities. These measures help to protect against data breaches, identity theft, and other cyber threats.

2) Privacy Protection:

By ensuring the security of personal data, digital identity systems also protect user privacy. Secure systems prevent unauthorized access to personal data, helping to maintain user privacy and trust.

3) Innovation and Progress:

The Law of Security also has implications for innovation and progress in digital identity. It encourages the development and adoption of new security technologies and practices, driving progress in the field and creating new areas of growth to address accelerating needs.

C. Challenges and Considerations

Implementing the Law of Security in digital identity systems comes with its own set of challenges and considerations:

1) Balancing Security and Usability

One of the biggest challenges in implementing the Law of Security is balancing security with usability. While strong security measures are crucial, they should not come at the expense of user experience. For example, complex authentication methods may enhance security but could also frustrate users and lead to poor adoption rates.

2) Keeping Up with Evolving Threats

The cybersecurity landscape is constantly evolving, with new threats emerging regularly. Digital identity systems must be able to adapt and respond to these changing threats, which require continuous monitoring, updates, and improvements.

3) Cost of Implementation

Implementing robust security measures can be costly. This includes the cost of developing and maintaining the security infrastructure and regular updates and patches. Organizations must consider these costs when designing and implementing digital identity systems.

4) Governing Compliance

Different authorities have different regulations regarding data security. Digital identity systems must be designed to comply with all relevant regulations, which can be a complex and challenging task, especially for global systems that operate across multiple jurisdictions.

5) Privacy Considerations

While security measures are designed to protect user data, they must also respect user privacy. For example, biometric authentication methods can enhance security but also raise privacy concerns. Digital identity systems must navigate these considerations carefully.

6) Education and Awareness

Users play a crucial role in the security of digital identity systems. However, many users are unaware of the risks associated with poor security practices. Educating users about these risks and how to protect their digital identities is a significant challenge.

Ensuring security in a digital context can be complex, due to the evolving nature of cyber threats and the technical challenges associated with securing copious amounts of data.

VI. Law 5: The Law of Transparency

The fifth law in our modern identity framework is the Law of Transparency. This law asserts that digital identity systems should operate in a transparent manner, providing individuals with clear information about how their personal data is collected, used, and shared.

A. Understanding Transparency

Transparency in the context of digital identity refers to the openness and clarity with which a system operates. A transparent digital identity system provides individuals with clear, understandable information about its data practices, including what data is collected, how it is used, who it is shared with, and how long it is retained. Transparency also involves providing individuals with information about their rights and how they can exercise them.

B. Implications of the Law of Transparency

The Law mandates that these systems should be designed with transparency in mind, incorporating features such as clear privacy notices, user-friendly interfaces, and mechanisms for individuals to access, correct, and delete their personal data.

1) Informed Consent

The Law of Transparency supports informed consent by ensuring that users have the information they need to make informed decisions about their data. This includes information about what data is collected, how it is used, who it is shared with, and how it is protected.

2) Accountability

Transparency promotes accountability by making it clear who is responsible for various aspects of the digital identity system. This includes who is responsible for collecting and storing data, who is responsible for protecting it, and who is responsible for any data breaches or privacy violations.

By providing individuals with clear information about their data, it empowers them to make informed decisions about their digital identities. And by promoting openness and accountability, it enhances trust in the system and discourages misuse of data.

C. Challenges and Considerations

Communicating complex data practices in a clear, understandable manner can be challenging. We have seen this though the implementation of the General Data Protection Regulation or GDPR where systems globally began to address the needs of disclosure and transparency. Some areas of consideration:

1) Complexity of Information

Digital identity systems can be complex, and explaining how they work in a clear and understandable way can be challenging. It is important to strike a balance between providing comprehensive information and ensuring that this information is accessible to users with varying levels of technical understanding.

2) Changing Practices

As digital identity systems evolve and change, so must the information provided to users too. Keeping transparent information up to date can be a significant challenge, particularly for complex and rapidly evolving systems.

3) Legal Compliance

Different jurisdictions have different requirements for transparency. Ensuring compliance with all relevant laws and regulations can be a complex task, particularly for global systems that operate across multiple jurisdictions.

4) User Engagement

While transparency is crucial, it is also important to ensure that users engage with the information provided. Many users do not read or understand privacy policies and other transparent information. Encouraging user engagement with transparency information is a significant challenge.

5) Balancing Transparency and Security

While transparency is important, it must be balanced with security. Providing too much information about the inner workings of a digital identity system could potentially provide a roadmap for malicious actors. Striking the right balance between transparency and security is a key consideration.

Furthermore, the Law of Transparency requires careful balancing with other considerations, such as security. For instance, while transparency is important, it should not compromise the security of the system by revealing sensitive information about its operation.

VII. Law 6: The Law of Attestations

The sixth law in our modern identity framework is the Law of Attestation. This law emphasizes that attestations, or claims made about an individual's identity, should be verifiable and trustworthy, ensuring the integrity of the identity system.

A. Understanding Attestation

Attestation in the context of digital identity refers to the process of confirming or validating a claim made about an individual's identity or attribute of an identity. An attestation could be a digital signature from a trusted authority confirming the validity of a document, a verification code sent to a user's phone to confirm their possession of the number, or a statement from a trusted source confirming an individual's credentials or qualifications. Individuals must be able to obtain and manage digital attestations of their personal information and credentials, such as educational degrees or professional certifications easily and securely.

B. Implications of the Law of Attestations

Furthermore, the Law of Attestation requires careful balancing with other considerations. For instance, while attestations can enhance the reliability of digital identities, they should not infringe on an individual's privacy or control over their personal data.

The Law of Attestation sets a high standard for the verification and trustworthiness of claims made in digital identity systems. However, realizing its full potential requires careful design and management of trust relationships, considering the challenges associated with ensuring the verifiability and trustworthiness of attestations. Some areas include:

1) Trust and Verification

The Law of Attestation enhances trust in digital interactions by allowing for the verification of claims or attributes. When individuals can prove certain aspects of their identity, it builds trust and facilitates online transactions.

2) Security

By allowing for the verification of claims, the Law of Attestation can enhance the security of digital identity systems. It can help to prevent identity fraud and other malicious activities.

3) User Attribute Management

choose which attributes to share and with whom. This can help to protect privacy and give users more control over their digital identities.

4) Inclusion

The Law of Attestation can promote social and economic inclusion. By providing a secure and reliable means of proving one's identity, digital identity systems can enable access to essential services such as banking, healthcare, and education, particularly for marginalized or underserved communities.

5) Interoperability:

The Law of Attestation supports interoperability by allowing for the verification of claims across different systems and entities. This can facilitate the use of digital identities across a wide range of services and applications.

C. Challenges and Considerations for the Law of Attestation

Ensuring the verifiability and trustworthiness of attestations can be complex, requiring robust mechanisms for digital signatures, secure communication, and third-party verification. It also requires careful management of trust relationships, to ensure that attestations are issued and accepted by trusted entities. Some areas to consider:

1) Verification Complexity

Verifying claims or attributes associated with an individual's identity can be complex, particularly when it involves sensitive or subjective information. This can make it challenging to implement effective attestation mechanisms.

2) Privacy Concerns

Attestation mechanisms must be designed in a way that respects user privacy. This includes ensuring that the verification process does not unnecessarily expose sensitive personal information.

3) Security Risks

The process of attestation can introduce security risks, such as the potential for identity theft or fraud. It's crucial to ensure that attestation mechanisms are secure and resistant to these types of threats.

4) User Experience

Attestation mechanisms must be user-friendly. If the process of attesting to one's identity is too complex or cumbersome, it could deter users and reduce the usability of the digital identity system.

VIII. Law 7: The Law of Equity

The seventh law is the Law of Equity. This law emphasizes that digital identity systems should be equitable, ensuring that all individuals, regardless of their geographical location, socio-economic status, or technical capabilities, have access to and can benefit from the system.

A. Understanding Equity

Equity in the context of digital identity refers to the fairness and inclusivity of the system. An equitable digital identity system is one that is accessible to all individuals and does not discriminate based on factors such as race, gender, age, socio-economic status, or geographical location. It also considers the varying technical capabilities of users, ensuring that the system is user-friendly and does not disadvantage those with limited technical skills or resources.

It mandates that these systems should be designed with inclusivity and accessibility in mind, incorporating features such as user-friendly interfaces, support for multiple languages, and mechanisms to accommodate users with disabilities.

B. Implications of the Law of Equity

The Law of Equity asserts that digital identity systems should be accessible and fair to all users, regardless of their socioeconomic status, geographical location, or technical proficiency. This law is crucial in ensuring that the benefits of digital identity systems are broadly shared and do not contribute to digital inequality. Implications of the Law of Equity include:

1) Universal Access

Digital identity systems must be designed to be accessible to all individuals, regardless of their location, economic status, or technical skills. This includes providing affordable access, user-friendly interfaces, and support for multiple languages and accessibility needs.

2) Inclusion

The Law of Equity implies that digital identity systems should promote social and economic inclusion. By providing a secure and reliable means of proving one's identity, digital identity systems can enable access to essential services such as banking, healthcare, and education, particularly for marginalized or underserved communities.

3) Non-Discrimination

Digital identity systems must be designed and operated in a way that does not discriminate against any user or group of users. This includes ensuring that the system does not unfairly disadvantage or exclude certain users based on their race, gender, age, disability, or any other characteristic.

4) User Empowerment

The Law of Equity also implies that users should have control over their digital identities. This includes the ability to decide who can access their data, for what purposes, and for how long, as well as the right to update, correct, or delete their data.

5) Transparency and Accountability

To ensure equity, digital identity systems must be transparent in their operations and accountable for their actions. This includes providing clear and accessible information about how the system works, how data is collected and used, and how decisions are made.

C. Challenges and Considerations

Requiring careful consideration of diverse user needs and capabilities, The Law of Equity, also requires ongoing monitoring and adjustment to ensure that the system remains equitable as user needs and circumstances evolve. Some areas to consider:

1) Accessibility

Ensuring that digital identity systems are accessible to all individuals, regardless of their location, economic status, or technical skills, can be a significant challenge. This includes providing affordable access, user-friendly interfaces, and support for multiple languages and accessibility needs.

2) Digital Divide

The digital divide — the gap between those who have access to technology and those who do not — is a major challenge for the Law of Equity. Efforts must be made to ensure that digital identity systems do not exacerbate this divide and that they are

accessible to individuals in all parts of the world, including rural and underprivileged areas.

3) Cultural Sensitivity

Diverse cultures have different perceptions and expectations about identity, privacy, and data sharing. Designing a digital identity system that respects these cultural differences and is fair and equitable to all users can be a complex task.

4) Laws and Regulations

Ensuring that a digital identity system complies with all relevant laws and regulations, and is equitable to users in different jurisdictions, can be a significant challenge.

5) User Education

Many users may not be aware of their rights and responsibilities in relation to their digital identities. Educating users about these issues and ensuring that they can exercise their rights and responsibilities in an equitable manner, is a key consideration.

Identity systems must be fair and equitable, and individuals must not be subject to discrimination or unequal treatment based on their personal information.

Furthermore, the Law of Equity requires careful balancing with other considerations, such as security and functionality. For instance, while accessibility features can enhance equity, they should not compromise the security of the system or its core functionality.

IX. Law 8: The Law of Interoperability

The eighth law in our modern identity framework is the Law of Interoperability. This law asserts that digital identity systems should be interoperable, enabling seamless interaction between different systems, platforms, and services.

A. Understanding Interoperability

Interoperability in digital identity refers to different identity systems' ability to work together. An interoperable digital identity system can communicate and exchange data with other systems, allowing individuals to use their digital identities across multiple platforms and services. This not only enhances user convenience but also promotes efficiency and innovation.

The Law of Interoperability has significant implications for the design and operation of digital identity systems. It mandates that these systems should be designed with interoperability in mind, incorporating features such as open standards, APIs, and data portability.

B. Implications of the Law of Interoperability

1) Ease of Use

The Law of Interoperability enhances the ease of use of digital identity systems. When systems are interoperable, users can use their digital identities across a wide range of services and applications, reducing the need for multiple identities or credentials.

2) Efficiency

The Law of Interoperability promotes efficiency. By allowing different systems to work together, it can reduce duplication of effort and make the digital ecosystem more efficient.

3) Inclusion

The Law of Interoperability can promote social and economic inclusion. By enabling digital identities to be used across a wide range of services, it can make these services more accessible to individuals, particularly those in marginalized or underserved communities.

4) Innovation

The Law of Interoperability can drive innovation. By creating a more interconnected digital ecosystem, it can enable new services and applications that leverage digital identities in novel ways.

5) Partnership Adherence

Many laws and regulations, particularly in sectors such as finance and healthcare, require systems to be interoperable to ensure partnerships are protected. By adhering to the Law of Interoperability, digital identity systems can help businesses comply with these requirements.

C. Challenges and Considerations

The law of Interoperability requires careful management of data privacy and security, to ensure that data exchange does not compromise the protection of personal data, while creating an open and seamless system to allow digital identities flexibility and portability while maintain trust in the system. Some areas to consider:

1) Technical Compatibility

One of the main challenges with interoperability is ensuring technical compatibility between different systems. This requires the use of standardized protocols and data formats, which can be complex to implement.

2) Security and Privacy

Interoperability can pose security and privacy risks. It's crucial to ensure that data is transferred securely between systems and that privacy is maintained during the transfer process.

3) Cost and Complexity

Implementing interoperability can be costly and complex, particularly for legacy systems that were not designed with interoperability in mind.

X. Law 9: The Law of User Control

The ninth law in our modern identity framework is the Law of User Control. This law emphasizes that digital identity systems should provide users with control over their personal data, including what is collected, how it is used, and who it is shared with.

A. Understanding User Control

User control in the context of digital identity refers to the ability of individuals to manage their personal data. A digital identity system that respects user control allows individuals to

decide what personal data is collected, how it is used, who it is shared with, and how long it is retained. It also provides mechanisms for individuals to access, correct, and delete their personal data. Individuals must have control over their personal information, including the ability to manage, delete, and transfer it as they see fit.

The Law mandates that these systems should be designed with user control in mind, incorporating features such as clear privacy settings, user-friendly interfaces, and mechanisms for data access, correction, and deletion.

B. Implication for the Law of User Control

This law is fundamental to the modern digital landscape, where personal data is often collected, stored, and used without the individual's knowledge or consent. Implications of the Law of User Control include:

1) Privacy Protection

By giving individuals control over their digital identities and personal data, the Law of User Control helps to protect user privacy. Users can decide what personal data to share, with whom, and for what purpose, thereby maintaining control over their personal information.

2) Trust and Verification

The Law of User Control can enhance trust in digital interactions. When individuals have control over their digital identities, they can verify their identity to others in a secure and reliable manner, enhancing trust in online transactions.

3) Informed Consent

The Law of User Control supports informed consent by ensuring that users have the information they need to make informed decisions about their data. This includes information about what data is collected, how it is used, who it is shared with, and how it is protected.

4) User Empowerment

The Law of User Control empowers users by giving them control over their digital identities and personal data. This can enhance user satisfaction and engagement with the digital identity system.

C. Challenges and Considerations

User control in a digital context requires careful design of user interfaces and also requires ongoing education and support to help users understand and exercise their data rights.

By providing individuals with control over their personal information, this law helps to reduce the risk of identity fraud and theft and increase privacy and security. Some areas to consider:

1) Usability

While giving users control over their digital identities is important, it must be balanced with usability. Too many controls or complex interfaces can make the system difficult to use, which could deter users and reduce adoption rates.

2) Education

Many users are not fully aware of the importance of controlling their digital identities or how to effectively use the controls provided. Educating users about these issues is a significant challenge.

3) Security

Giving users control over their digital identities can enhance security by reducing the amount of data held by any one entity. However, it also places more responsibility on the user to secure their own data, which can be a challenge if users are not familiar with best practices for data security.

4) Legal Rights and Laws

Compliance with all relevant laws and regulations can be a complex task, particularly for global systems that operate across multiple authorities.

5) Interoperability

For user control to be effective, digital identity systems must be interoperable with other systems and services. This can be a challenge, particularly in a fragmented digital landscape with many different systems and standards.

XI. Law 10: The Law of Data Minimization

The tenth law in our modern identity framework is the Law of Data Minimization. This law asserts that digital identity systems should collect, use, and retain only the minimum amount of personal data necessary to fulfill their purpose. A constrained and where necessary delegated approach will be required to address minimization.

A. Understanding Data Minimization

Data minimization in the context of digital identity refers to the principle that systems should limit the collection, use, and retention of personal data to what is strictly necessary. This includes collecting only the data needed to provide a service, using the data only for the purpose for which it was collected, and retaining the data only for as long as necessary to fulfill that purpose.

B. Implications of the Law of Data Minimizations

1) Privacy Protection

By limiting the amount of personal data collected and stored, the Law of Data Minimization helps to protect user privacy. The less data a system holds, the less opportunity there is for that data to be misused or exposed in a data breach.

2) Security

The Law of Data Minimization enhances security by reducing the amount of data that could potentially be exposed in a data breach. The less data a system holds, the less attractive it is as a target for hackers.

3) Efficiency

By collecting and storing only the necessary data, digital identity systems can operate more efficiently. This can reduce storage costs and improve system performance.

C. Challenges and Considerations

Ensuring data minimization in a digital requires careful design of data collection and management processes. It also requires ongoing monitoring and adjustment to ensure that data

practices remain aligned with the principle of data minimization. Some areas to consider:

1) Determining Necessary Data

One of the main challenges with data minimization is determining what data is "necessary." This can vary depending on the specific service or function the digital identity system is providing, and making this determination can be complex.

2) Balancing Functionality and Privacy

While minimizing data collection can enhance privacy, it must be balanced with maintaining the functionality of the digital identity system. Some services may require more data to function effectively, and striking the right balance can be challenging.

3) Data Retention Policies

Implementing data minimization also involves determining how long data should be retained. This requires creating and enforcing data retention policies, which can be a complex task.

4) User Expectations

Users may have different expectations about what data should be collected and how long it should be retained. Balancing these expectations with the principles of data minimization can be a challenge.

XII. Law 11: The Law of Data Portability

The eleventh law in our modern identity framework is the Law of Data Portability. This law asserts that digital identity systems should allow users to easily transfer their personal data from one system to another

A. Understanding Data Portability

Data portability in the context of digital identity refers to the ability of individuals to move, copy, or transfer their personal data easily from one environment or system to another. This includes the ability to export personal data in a structured, commonly used, and machine-readable format, and to import it into another system without hindrance.

B. Implications of the Law of Data Portability

Systems should be designed with data portability in mind, incorporating features such as data export and import functions, open data formats, and interoperable APIs.

1) User Data Sovereignty

The Law of Data Portability enhances data sovereignty by allowing individuals to move their data from one service to another. This can help users to avoid being locked into a particular service and gives them more freedom to choose the services that best meet their needs.

2) Competition

By making it easier for users to switch between services, the Law of Data Portability can promote competition. This can drive innovation, improve service quality, and lower prices.

3) Interoperability

The Law of Data Portability supports interoperability by requiring services to be able to export and import user data in a standardized format. This can facilitate the use of digital identities across a wide range of services and applications.

4) Government and Regional Compliance

Many privacy laws and regulations, for example GDPR in the EU, include requirements for data portability. By adhering to the Law of Data Portability, digital identity systems can help businesses comply with these requirements.

5) User Trust

The Law of Data Portability can enhance user trust by demonstrating that the digital identity system respects consent from users by providing freedom of choice.

C. Challenges and Considerations

Careful design of data export and import functions, and adherence to open data standards are core to the requirements necessary. It also requires careful management of data security and privacy, to ensure that data transfers do not compromise the protection of personal data. Some areas of consideration:

1) Technical Compatibility

One of the main challenges with data portability is ensuring technical compatibility between different service providers. This requires the use of standardized data formats and protocols, which can be complex to implement.

2) Security and Privacy

Transferring data between services can pose security and privacy risks. It is crucial to ensure that data is transferred securely, and that privacy is maintained during the transfer process.

3) User Understanding and Control

Users need to understand what data portability means, how to use it, and what the implications are for their data. Educating users about these issues and providing them with easy-to-use data portability tools is a significant challenge.

4) Legal and Regulatory Compliance

Ensuring compliance with all relevant laws and regulations can be a complex task, particularly for global systems that operate across multiple jurisdictions.

5) Data Integrity

When data is transferred between services, it is important to ensure that the integrity of the data is maintained. This includes ensuring that the data is not corrupted or altered during the transfer process.

XIII. Law 12: The Law of Auditability

The twelfth law in our modern identity framework is the Law of Auditability. This law asserts that digital identity systems should be auditable, providing mechanisms for checking and verifying the system's operations and data practices.

A. Understanding Auditability

Auditability in the context of digital identity refers to the ability to review, inspect, and verify the operations of a system. An auditable digital identity system provides mechanisms for checking its operations, such as logs of data access and

modifications, and tools for verifying its data practices, such as privacy impact assessments and third-party audits.

The Law of Auditability mandates that these systems should be designed with auditability in mind, incorporating features such as logging, monitoring, alerting, and querying that enables auditing capabilities. This is achieved using transparent and auditable systems that allow individuals to monitor the use of their personal information and to ensure that it is being used in accordance with their preferences.

B. Implications of the Law of Auditability

The Law of Auditability posits that digital identity systems should be designed in a way that allows for independent verification of their operations and practices. This law is crucial for ensuring trust, accountability, and transparency in digital identity systems.

1) Trust

The Law of Auditability enhances trust in digital identity systems. When systems can be audited and their operations verified, it builds confidence among users and stakeholders that the system is operating as intended and that it adheres to its stated policies and standards.

2) Accountability

The Law of Auditability promotes accountability. By allowing for independent verification of operations, it ensures that digital identity systems are held accountable for their actions and practices.

3) Transparency

The Law of Auditability supports transparency. Audits can provide insights into how a digital identity system operates, including how it collects, uses, and protects personal data.

4) Regulatory Compliance

Many laws and regulations require businesses to be able to demonstrate compliance through audits. By adhering to the Law of Auditability, digital identity systems can help businesses meet these requirements.

5) Security

The Law of Auditability can enhance security. Regular audits can help to identify and address potential security vulnerabilities, thereby enhancing the overall security of the digital identity system.

C. Challenges and Considerations

Careful design of logging and monitoring systems, and robust mechanisms for third-party audits will be necessary. The Law also requires careful management of data security and privacy, to ensure that auditing processes do not compromise the protection of personal data. Some Areas to Consider:

1) Technical Complexity

Auditing a digital identity system can be technically complex, requiring specialized knowledge and skills. This can make it challenging to find qualified auditors and to conduct thorough and effective audits.

2) Security and Privacy

Conducting an audit involves accessing and analyzing sensitive system data, which can pose security and privacy risks. It's crucial to ensure that audits are conducted in a way that maintains the security and privacy of the system and its users.

3) Cost

Conducting regular audits can be costly. This includes the cost of hiring qualified auditors, the time required to conduct the audit, and any costs associated with addressing identified issues or vulnerabilities.

4) Transparency vs. Security

While audits can enhance transparency, they must be balanced with security. Providing too much information about the inner workings of a digital identity system could potentially provide a roadmap for malicious actors. Striking the right balance between transparency and security is a key consideration.

Furthermore, the Law of Auditability requires careful balancing with other considerations, such as system performance and user privacy. For instance, while logging and monitoring can enhance auditability, they should not compromise the performance of the system or the privacy of users.

XIV. Importance of Proactive Corporate and Government Participation

The successful implementation of the Modern Identity Laws hinges significantly on the proactive participation and sponsorship of both corporate entities and government bodies. Their involvement is crucial for several reasons:

A. Policy Making and Regulation

Governments play a pivotal role in setting the legal and regulatory framework for digital identity systems. By proactively endorsing and implementing the Modern Identity Laws, governments can create a conducive environment that encourages the development of secure, privacy-respecting, and user-centric digital identity systems. They can also ensure that these laws are reflected in national and international regulations, thereby promoting their widespread adoption.

B. Resource Allocation

Both corporate entities and governments have the resources necessary to develop and implement robust digital identity systems. Their financial support can accelerate the development of technologies and infrastructure needed to realize the Modern Identity Laws.

C. Public Trust

The endorsement and active participation of reputable corporate entities and government bodies can enhance public trust in digital identity systems. This is particularly important given the sensitive nature of identity data and the potential risks associated with its misuse.

D. Innovation and Collaboration

Corporate entities, with their capacity for innovation, can contribute significantly to the development of new technologies and solutions that embody the Modern Identity Laws. Moreover, collaboration between different corporate entities, as well as

between the corporate sector and government, can lead to the development of interoperable systems that enhance user convenience and promote the widespread use of digital identities.

E. Equity and Inclusion

Governments, in particular, have a responsibility to ensure that digital identity systems are accessible to all citizens, including marginalized and underserved communities. By proactively implementing the Modern Identity Laws, governments can promote equity and inclusion in the digital identity landscape.

XV. Conclusion and Future Directions

The 12 Modern Identity Laws provide a comprehensive framework for designing and implementing identity systems that are secure, private, and equitable. By adopting these laws, we can create an ecosystem of identity systems that empowers individuals to control their own digital identity and manage their personal information in a secure and transparent manner. This will help to reduce the risk of identity fraud and theft, increase privacy and security, and promote equity and accessibility for all individuals.

The digital identity landscape is rapidly evolving, driven by technological advancements, changing user needs, and regulatory developments. Moving towards a future where digital identities become increasingly central to our lives, it is crucial to ensure that these identities are secure, private, user-controlled, and interoperable. As digital interaction continues to grow, these laws will only become more pertinent.

The journey towards this future is not without challenges. Ensuring privacy and security, promoting user control and consent, achieving interoperability, and complying with regulations are complex tasks that require ongoing effort and collaboration.

The implementation of these laws will require collaboration between governments, organizations, and individuals to ensure that identity systems are designed and implemented in a way that is secure, private, and equitable. This will require the adoption of open standards and protocols and the development of modern technologies and systems in line with the 12 Modern Identity Laws' principles.

Furthermore, institutions and corporations set to benefit from being good corporate citizens by protecting and utilizing identity in a manner that reduces the detrimental monetary impacts to their business while still securing their user's information. The business benefit is in the billions if done collaboratively.

Looking ahead, digital identity will continue to be a key focus for businesses, governments, and individuals. As we navigate this landscape, there is hope that the 12 Modern Identity Laws will serve as a guide, helping us to create digital identity systems that are fit for the future.

Glossery of Key Terms

The following section provides definitions of key terms relevant to our discussion on digital identity systems.

Consent: Consent, in the context of digital identity, refers to explicit permission given by users for certain actions to be taken with their personal data. This often takes the form of clear, affirmative action – such as ticking a box or clicking a button.

Zero-Knowledge Proof (ZKP): ZKP is a cryptographic method where one party (the prover) can prove to another party (the verifier) that they know a specific piece of information, without conveying any information apart from the fact that they know it. In digital identity systems, ZKPs can be used to verify identity attributes without revealing the attributes themselves.

Data Breach: A data breach is an incident where unauthorized individuals gain access to confidential data. In the context of digital identity, a data breach may lead to exposure of personal identity attributes, leading to potential identity theft or other forms of exploitation.

P**seudonymous Identity:** A pseudonymous identity is a digital identity where the user's real-world identity is not linked to their online activities. Instead, a pseudonym or alias is used. While pseudonymous identities can provide a degree of privacy, they can also be linked back to real-world identities through techniques like data correlation and analysis.

User-Centric Design: A design philosophy that places the needs, preferences, and abilities of the user at the forefront of the design process. In digital identity systems, user-centric design ensures that systems are intuitive, accessible, and efficient for the people who use them.

Transparency: Transparency refers to the clarity and openness of operations. In digital identity systems, transparency involves making the system's workings and policies clear to users and other stakeholders. This may involve disclosing how personal data is used, who has access to it, and what measures are in place to protect it.

Open Standards: Open standards are publicly available standards developed through a collaborative process. They are free for anyone to use and typically developed and maintained by standards organizations. In digital identity systems, open standards facilitate interoperability and ensure wider adoption. Examples include OAuth and OpenID Connect.

Immutability: unchanging over time or unable to be changed

Implications: the effect that an action or decision will have on something else in the future.

References

[1] John Buzzard, "2023 Identity Fraud Study: The Butterfly Effect," 28 03 2023. [Online]. Available: https://javelinstrategy.com/research/2023-identity-fraud-study-butterfly-effect. [Accessed 01 07 2023].

[2] Javelin Strategy & Research, "Identity Fraud Losses Total $52 Billion in 2021, Impacting 42 Million U.S. Adults," 29 03 2022. [Online]. Available: https://javelinstrategy.com/press-release/identity-fraud-losses-total-52-billion-2021-impacting-42-million-us-adults. [Accessed 05 06 2023].

[3] Aite Group, "U.S. Identity Theft: The Stark Reality," 09 03 2021. [Online]. Available: https://aite-novarica.com/report/us-identity-theft-stark-reality. [Accessed 24 09 2022].

[4] B. AUXIER, M. ANDERSON, A. PERRIN, M. KUMAR and E. TURNER, "Americans concerned, feel lack of control over personal data collected by both companies and the government," PEW RESEARCH CENTER, 15 11 2019. [Online]. Available: https://www.pewresearch.org/internet/2019/11/15/americans-concerned-feel-lack-of-control-over-personal-data-collected-by-both-companies-and-the-government/. [Accessed 20 06 2023].

[5] Ponemon Institute & IBM Security, "Cost of a Data Breach Executive Summary," IBM Security, 2022.