SELF-SOVEREIGN IDENTITY: THE HARMONISING OF DIGITAL IDENTITY SOLUTIONS THROUGH DISTRIBUTED LEDGER TECHNOLOGY

JONATHAN LIM*

ABSTRACT

The purpose of this article is to highlight existing trust policy issues associated with the creation and use of digital identity systems. Doing so must be considered a precondition to fully realising the opportunities provided by distributed ledger technology in creating a permission-less, interoperable and decentralised digital identity framework under Self-Sovereign Identity ('SSI'). The approach adopted illustrates the importance of the 10 guiding principles of SSI in creating certainty and uniformity in its adoption, reviews the Trust Over Internet Protocol ('TOIP') stack as a blueprint for policy interoperability and analyses the need for legal compliance in creating a trust policy framework. It is established that a consideration of cross-jurisdictional data and privacy laws, along with the implementation of foundational legal principles, is necessary to create a trust policy framework. To introduce a robust and trusted digital identity, this paper suggests that policymakers consider the application of legal principles and values in addressing underlying and persisting policy deficiencies.

I INTRODUCTION

The realisation of Self-Sovereign Identity ('SSI') via the use of distributed ledger technology ('DLT') provides individuals with the possibility of greater control and security over their personal identity; however, the formation of an underlying trust framework is necessary if a robust digital identity solution is to be created. The law has often struggled to keep up with advances in technology.[1] The adoption of SSI as a definitive digital identity solution is challenged by the need for clarification in respect to the governance and regulatory aspects attached to any SSI trust policy framework ('TPF').

The increasingly digitalised environment within which individuals interact, coupled with the mass proliferation of digital services, has given rise to an increasingly chaotic and unsecure identity ecosystem. The disparate, centralised identity systems maintained by numerous governments have been proven to be inefficient, incompatible, lacking in privacy controls and

* Jonathan Lim is a cybersecurity analyst and solicitor at WiseLaw, where he advises clients on privacy, ICT and cyberlaw matters. He also volunteers his expertise as a human rights specialist at the Internet Bar Organization, advising on The Invisibles project - building digital identity for refugees and making technology work for justice.

[1] Lyria Bennett Moses, 'Agents of Change: How the Law Copes with Technological Change' (2011) 20(4) *Griffith Law Review* 763, 763.

vulnerable to cyber-attacks.[2] This was observed during the 2018 data breach of India's Aadhaar, the world's largest biometric identification system that resulted in the theft of the personal data of more than 1 billion people.[3] Individuals have increasingly fallen victim to the forceful fragmentation of their personal information and data across various service providers that rely on access and reference to an individual's identity to deliver services and drive profit. This has led to large amounts of identity data being duplicated onto the servers of authorities,[4] granting service providers the unparalleled authority to authenticate and/or revoke a person's digital identity.[5]

The ubiquity of DLT in the management of digital assets provides opportunities to realise the creation of a safe, secure and trusted digital identity framework. DLT represents a decentralised database that eliminates the need for a central authority to process, validate, or authenticate transactions.[6] DLT provides a trust solution that encompasses enhanced security, transparency and permanence. This provides an underlying platform for commerce, identity or ownership.[7] Blockchain represents a subset of DLT that is distinguished by its use of cryptographic signing and linking groups of records in a ledger to form a chain and create a tamper-proof log of sensitive activity.[8]

The specific application of blockchain in digital identity management provides greater control to the individual over their biometric data and personal information, as it enables the individual to decide what information is disclosed, to whom and under what circumstances.[9] This is predicated upon the requirement that digital identities are not locked into any given platform or controlled by a centralised authority, but remain portable and interoperable across multiple

[2] John Callahan, 'Self-Sovereign Biometrics and the Future of Digital Identity', *CSO Australia* (online at 5 March 2018) <https://www.csoonline.com/article/3259889/self-sovereign-biometrics-and-the-future-of-digital-identity.html>.

[3] Ashish Malhotra, 'The World's Largest Biometric ID System Keeps Getting Hacked', *Vice* (online at 9 January 2018) <https://www.vice.com/en_us/article/43q4jp/aadhaar-hack-insecure-biometric-id-system>.

[4] Quinten Stokkink and Johan Pouwelse, 'Deployment of a Blockchain-Based Self-Sovereign Identity', *arXiv* (Submission, 5 June 2018) <https://arxiv.org/abs/1806.01926> 1337.

[5] Joseph Culter et al, 'Self-Sovereign Identity and Distributed Ledger Technology: Framing the Legal Issues', *PerkinsCoie* (Web Page, May 2017) <https://www.perkinscoie.com/en/news-insights/self-sovereign-identity-and-distributed-ledger-technology.html> 1.

[6] Oliver Belin, 'The Difference Between Blockchain and Distributed Ledger Technology', *TradeIX* (Web Page, 2020) <https://tradeix.com/distributed-ledger-technology/>; Sinclair Davidson et al, 'Blockchains and the Economic Institutions of Capitalism' (2018) 14(4) *Journal of Institutional Economics* 639, 642.

[7] Douglas W Arner et al, *Distributed Ledger Technology and Digital Assets—Policy and Regulatory Challenges in Asia* (Asian Development Bank Report, 2019) 9.

[8] World Bank, 'Blockchain and Distributed Ledger Technology (DLT)', *World Bank* (Web Page, 12 April 2018) <https://www.worldbank.org/en/topic/financialsector/brief/Blockchain-dlt>.

[9] Wolfond Greg, 'A Blockchain Ecosystem for Digital Identity: Improving Service Delivery in Canada's Public and Private Sectors' (2017) 7(10) *Technology Innovation Management Review* 35, 35.

platforms—elements that intersect with SSI.[10] Tied to this is the issue of privacy and data protection. Specifically, issues arise as to how data protection concepts and rules will apply to blockchain, and questions arise as to whether the creation of compliant blockchain applications involving the processing of consumers' personal data is even possible.[11]

The proliferation of data and privacy laws in Europe over the past decade demonstrates a growing awareness among policymakers surrounding the vulnerable state of digital infrastructure and the questionable practices of internet companies.[12] This has given rise to a demand for greater control over our identities and personal information.[13] Similarly, in Australia, there has been a move towards protecting individual privacy rights in the context of consumer affairs, where providing consumers with greater control over data has become an increasing policy priority. This was highlighted in the Australian Government's response to the Australian Competition and Consumer Commission's ('ACCC') Digital Platform Inquiry of December 2019.[14]

Blockchain exists as a means of pioneering the path to SSI through its decentralised nature, use of public-key encryption to enhance security and by building trust in online services. SSI exists as an elegant solution that provides a 'lifetime portable digital identity that does not depend on any central authority and can never be taken away'.[15] Blockchains do not eliminate trust, but minimise the amount of trust required from any single actor in the system by broadly distributing such trust. SSI has been primarily characterised by its trust-less and decentralised nature;[16] however, it is also defined by its need for legal clarity. Such clarity is necessary if its formal and widespread adoption is to be supported by governments and the business sector.[17]

SSI represents both a framework and digital movement that recognises the individual's right to own and control their identity without reliance upon a government or a centralised

[10] Fennie Wang and Primavera De Filippi, 'Self-Sovereign Identity in a Globalised World: Credentials-Based Identity Systems as a Driver for Economic Inclusion', *Frontiers in Blockchain* (online at 23 January 2020) <https://www.frontiersin.org/articles/10.3389/fbloc.2019.00028/full>.

[11] Christopher Kuner et al, 'Blockchain Versus Data Protection' (2018) 8(2) *International Data Privacy Law* 103.

[12] Josh Constine, 'A Flaw-By-Flaw Guide to Facebook's New GDPR Privacy Changes', *TechCrunch* (online at 18 April 2018) <https://techcrunch.com/2018/04/17/facebook-gdpr-changes/>.

[13] Bojan Siminc, 'Can Blockchain Solve Identity Fraud?', *Forbes* (online at 31 May 2018) <https://www.forbes.com/sites/forbestechcouncil/2018/05/31/can-Blockchain-solve-identity-fraud/#77aab4cb7289>.

[14] Australian Competition and Consumer Commission, 'ACCC Digital Platforms Inquiry', *ACCC* (9 January 2020) <https://www.accc.gov.au/about-us/tools-resources/social-media/transcripts/accc-digital-platforms-inquiry>.

[15] Vinod Baya, 'Digital Identity: Moving to a Decentralised Future', *Citi* (Blog Post, 9 October 2019) <https://www.citi.com/ventures/perspectives/opinion/digital-identity.html>.

[16] Alexander Muhle et al, 'A Survey on Essential Components of a Self-Sovereign Identity', *ResearchGate* (online at July 2018) <https://www.researchgate.net/publication/326459642_A_Survey_on_Essential_Components_of_a_Self-Sovereign_Identity>.

[17] Ian Hall, 'EU Report Signposts Route to Blockchain ID Verification' *Global Government Forum* (Report, 30 May 2019) <https://www.globalgovernmentforum.com/eu-report-signposts-route-to-blockchain-id-verification/>.

authority.[18] In approaching SSI and blockchain, one must move beyond the question of *how* we could digitise existing features of identity management to consider the legal elements of the TPF for digital identity.

II Context

A *Conceptualising Digital Identity*

Civil society groups, such as the Internet Identity Workshop, have recognised the potential of elevating digital identity under SSI through the use of blockchain technology.[19] A trusted identity could span both the physical and digital context. Accordingly, 'digital identity' is defined as the online presence that represents and acts on behalf of an external actor in an ecosystem[20] and thus is the unique representation of a subject engaged in an online transaction.

Ideally, one's identity and digital identity would be verified by a trust anchor within the SSI framework. Trust anchors represent a collection of entities (eg, governments and banks) with properly aligned incentives to tell the truth, as opposed to a single entity in a centralised system.[21] Under the traditional identity framework, governments and financial institutions have assumed this role by providing citizens with identity documents, such as passports or drivers' licences. Given the contemporary tenuous nature of trust between citizens and their governments in relation to privacy and technology, the growing capabilities of civil society and industry organisations may bridge this trust gap as trust anchors in this new digital identity ecosystem.[22]

Trust anchor organisations can confirm the legitimacy of an actor and provide those interacting with the actor confidence in the authenticity of their identity credentials.[23] These entities can authenticate your digital identity through identity documents and create identity documents using biometrics; thus, a person can be identified and authenticated based on a set of

[18] Abdulrahman Fahad Sindi, 'Adoption Factors of a Blockchain Digital Identity Management System in Higher Education: Diffusing a Disruptive Innovation' *ProQuest* (online at 2019) 9 <https://search.proquest.com/openview/a85e5edc48014246f9eb1d93ede6e535/1.pdf?pq-origsite=gscholar&cbl=18750&diss=y>.

[19] 'Kaliya Young Interview (Co-Founder of the Internet Identity Workshop and Author of the Domains of Identity)', *TyKn* (Web Page, 16 October 2019) <https://tykn.tech/interview-with-kaliya-young/>.

[20] 'Digital Identity — Overview', *World Economic Forum* (Web Page, 2020) <http://widgets.weforum.org/Blockchain-toolkit/digital-identity/#building-trusted-digital-identities>.

[21] Jose van Dijck and Bart Jacobs, 'Electronic Identity Services as Sociotechnical and Political–Economic Constructs' (2019) 22(5) *New Media and Society* 896, 898.

[22] Chris Burt, 'Civil Society and Industry Tackle Issues with Biometrics and Digital ID for Social Development', *BiometricUpdate.com* (online at 11 June 2019) <https://www.biometricupdate.com/201906/civil-society-and-industry-tackle-issues-with-biometrics-and-digital-id-for-social-development>.

[23] 'Blockchain and Biometrics: The Future of Identity', *Veridium* (Web Page, 25 May 2018) <https://veridiumid.com/future-identity-Blockchain-biometrics/>.

recognisable and verifiable data that is unique and specific to the individual.[24] A digital identity comprises several different elements, which collectively relate to the traits of SSI:[25]

A) Registration Information—Copies of a governmental or other officially issued documents provided at registration for a service.

B) Transactional Identity—The set of facts required to re-authenticate a user before a transaction will be permitted in a particular system and time.

C) Transaction History—The list of transactions in a system over time.

D) Digital History—The combination of transactions conducted in a system and information retained by the system about each user conducting those transactions.

A person's digital identity comprises a set of digital histories across systems relating to a single legal identity.[26] It is not a simple documentation of or medium transition of a person's non-digital identities.[27] For a digital identity to meet the needs of governments, businesses and individuals, it must be personal, persistent, portable and private.[28] Consequently, within the context of a blockchain, a digital identity can be understood as a digital asset (ie, a representation of something of value for which ownership is verified and recorded on a distributed ledger).

However, accessing a digital service may not mean that the subject's real-life identity is known, which can give rise to identity fraud issues.[29] The term secure (or trusted) digital identity integrates the requirements of privacy and trustworthiness — holding each party accountable in a transaction, proving a means by which one may identify the parties responsible for any specified part of a transaction. This means of attribution enables transactions and the creation of binding legal agreements in the digital world via the use of digital signatures. Accordingly, the creation, authentication and use of a trusted identity becomes more crucial in a digital environment absent face-to-face interactions between the parties.

[24] 'What is Biometrics?' *Thales* (Web Page, 15 May 2020) <https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics>.

[25] Alex Matthews and Catherine Tucker, 'Blockchain and Identity Persistence' in Chris Brummer (ed), *Cryptoassets: Legal, Regulatory and Monetary Perspectives* (Oxford University Press, 2019) 246.

[26] Alexis Margaret Wallace, 'Legal Identity in Australia', (PhD thesis, The University of Sydney, 1 February 2016) <https://ses.library.usyd.edu.au/handle/2123/15528>.

[27] Matthews and Tucker (n 25).

[28] World Economic Forum, 'The Known Traveller—Unlocking the Potential of Digital Identity for Secure and Seamless Travel', *Accenture* (January 2018) 23 <https://www.accenture.com/_acnmedia/PDF-70/Accenture-WEF-The-Known-Traveller-Digital-Identity.pdf>.

[29] Ibid 22.

B *The Evolution of Digital Identity*

Comprehending the potential of SSI as a sensible digital identity solution requires a consideration of the four phases identified by Christopher Allen in relation to the evolution of digital identity towards SSI.[30] The first phase of the evolution was centralised identity.[31] This stage involves administrative control by a single authority that acts as the issuer and authenticator of digital identity. This model results in information being siloed and fragmented across disparate online services, websites and applications. Consequently, the user does not own their digital identity and has little control over how it is used or shared by the authority. Under the second phase, a federated identity model is characterised by administrative control by multiple federated authorities, such that the user's online identity is debalkanised by a variety of commercial organisations.[32] This allows a person to use the same credentials to log in to multiple services; however, their identity is still controlled by each individual service provider. Thus, multiple authorities have the ability to restrict or remove the use of a person's digital identity credentials. Under the third phase, user-centric identity is described as being subject to individual or administrative control by multiple authorities; however, no federation is required. User-centric methodologies tend to focus on user consent and interoperability with the intent of providing a fully portable, user-controlled and secure digital identity service. This is achieved by separating the identity component from the rest of the application. However, users' digital identities are still maintained and controlled by the entities that provide the digital identity services. Finally, under the fourth phase, SSI provides a fully user-controlled and decentralised digital identity model across any number of authorities. In supporting user autonomy, the user must be considered central to the administration of the identity. This is achieved by ensuring that the user's identity is interoperable across multiple locations and enabling true user control of that digital identity.

C *Defining Self-Sovereign Identity*

SSI refers to the concept of individuals or organisations having sole ownership over their digital identities and control over how their data is shared and used, including who has access to, can refer to and who can share components of their identity. Certain components of identity are grounded by the issuing authorities (eg, passports and drivers' licences); however, the individual

[30] Culter et al (n 5) 2–3.

[31] Christopher Allen, 'The Path to Self-Sovereign Identity', *Coindesk* (Blog Post, 27 April 2016) <https://www.coindesk.com/path-self-sovereign-identity>.

[32] Christopher Allen, 'The Path to Self-Sovereign Identity', *Life With Alacrity* (Blog Post, 25 April 2016) <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>.

must consent to the sharing of their identities and any related data in every instance. This process is achieved by individuals securely storing their identity data on their own personal devices and providing it efficiently to those who need to validate it, without relying on a central repository of identity data and a single authority.[33]

To be truly in control of our personally identifiable information ('PII') or self-sovereign, an individual must have control over the cryptographic keys that enable access to their own digital identity data. When these cryptographic keys are integrated into a blockchain as a means of proving that you have the credentials, this opens new possibilities; for example, a person could verify their information on the blockchain ledger rather than have point-to-point contact with an individual or organisation.

A precise definition of what constitutes a SSI does not currently exist; however, a series of criterion have been identified as the underpinning principles of SSI. These guiding principles were first conceived by entrepreneur and technologist Christopher Allen in 2016 as a preliminary benchmark for SSI.[34] These principles may be interpreted as a means of setting legal standards and guidelines concerning what cumulative qualities of a system gives rise to its classification as an SSI framework for the benefit of legal certainty.[35] By leveraging a personalised blockchain structure, it is clear that several of these guiding principles are intrinsically fulfilled.[36] The guiding principles are as follows:

1. Existence—Individuals must have an independent existence (ie, they must exist independently of the digital identifiers that merely serve as a reference to them).

2. Control—Individuals must control their identities; they should always be able to refer to, update or even hide their identities, even if others can make claims about these identities.

3. Access—Individuals must have access to all the data related to their identities and should be able to retrieve their claims whenever needed.

[33] Antony Lewis, 'A Gentle Introduction to Self-Sovereign Identity', *Bits on Blocks* (Web Page, 17 May 2017) <https://bitsonblocks.net/2017/05/17/a-gentle-introduction-to-self-sovereign-identity/>.
[34] Allen (n 31).
[35] Robert A Schwinger, 'Blockchain Law: Liability Rumblings Along the Blockchain' (2019) 262 (11) *New York Law Journal* <https://www.nortonrosefulbright.com/en/knowledge/publications/351bb245/Blockchain-law-liability-rumblings-along-the-Blockchain>; Stokkink and Pouwelse (n 4) 1337; 'Self-Sovereign Identity' *P2P Foundation* (Web Page, 2020) <https://wiki.p2pfoundation.net/Self-Sovereign_Identity>; Metadium, 'Introduction to Self-Sovereign Identity and Its 10 Guiding Principles' *Medium* (Blog Post, 10 January 2019) <https://medium.com/metadium/introduction-to-self-sovereign-identity-and-its-10-guiding-principles-97c1ba603872>.
[36] Stokkink and Pouwelse (n 4) 1337.

4. Transparency—Systems and algorithms used to administer and operate digital identities must be open and transparent in terms of both their operation and maintenance.

5. Persistence—Identities must be long lived; preferably they should last forever or at least for as long as the user wishes to maintain them.

6. Portability—Information and services about identity must be transportable and must not be held by a single third-party entity, even if it is a trusted entity.

7. Interoperability—Identities should be as widely usable as possible, as opposed to being framed only to work in siloed environments.

8. Consent—Individuals must agree to the use of their identities; the sharing of user data must only occur with the consent of the data subject.

9. Minimisation—The disclosure of claims must be limited to the minimum necessary to accomplish the task at hand.

10. Protection—The rights of users must be protected at any cost, even if doing so would counter the interests of the identity providers.

The benefits of SSI revolve around its anonymity, pseudonymity, legal identity and versatility as a 'single source' and multi-verifier SSI. Most notable is its utility in simplifying Know Your Customer processes, in boosting and strengthening compliance with legal requirements through the elimination of intermediaries and in ensuring cryptographically provable verification and consent.[37]

The connection between SSI and the TPF is based on the need to bridge the trust gap between technology operators and end-stage users. From a technical perspective, it is clear that privacy by design has been a core consideration within the creation of SSI. Despite such assurances, the human element remains a core ethical concern, given the propensity for those in positions of authority to abuse technology for personal gain, which has resulted in persisting concerns surrounding the 'fear of misuse'. [38] Consequently, the development of a TFP aims to reinforce the SSI's privacy-by-design model from a policy and legal perspective.

[37] Timothy Ruff, 'The Three Models of Digital Identity Relationships', *Medium* (Blog Post, 25 April 2018) <https://medium.com/evernym/the-three-models-of-digital-identity-relationships-ca0727cb5186>.

[38] Arend Hintze, 'What an Artificial Intelligence Researcher Fears about AI', *The Conversation* (14 July 2017) <https://theconversation.com/what-an-artificial-intelligence-researcher-fears-about-ai-78655>.

1 *Applications of Self-Sovereign Identity*

The adoption of SSI offers significant socioeconomic benefits in supporting the enforcement of international human rights law. Currently 1.1 billion people live without an official identity;[39] however, the absence of an officially recognised identity hinders their access to basic social services and their ability to fully realise and enjoy basic human rights as per the International Covenant on Economic, Social and Cultural Rights ('ICESCR').

As a permanent, immutable ledger on a decentralised network, blockchain enables civil society groups and International Governmental Organisations to construct a framework for describing blockchain-based digital identity and to promote self-determination via its implementation across vulnerable communities.[40] Within the humanitarian sector, the promotion of SSI provides a promising solution to a wide range of persistent challenges, including those related to the power dynamics between users and the organisations that serve them and transparency in tracing global supply chains. Possible applications of DLT-based identification systems include cash transfer programs, the identification of refugees and stateless persons, land registration and titling and healthcare services.[41] SSI could thus restore the identities of stateless refugees, promote the credentialing of educational certifications and support the administration of welfare services by providing a form of digital identity that allows a sovereign form of self-determination and authentication of credentials.[42]

The concept of digital citizenship provides disadvantaged groups and countries with greater access to human rights and the global economy.[43] A properly designed and implemented SSI could offer such benefits while also protecting individuals from the ever-increasing control of those in power. One civil society project directed at addressing these issues is that of 'The Invisibles' at the Internet Bar Organization. This project is committed to establishing the

[39] Inclusivity '1.1 Billion People without Official Identity (Id)', *Inclusivity* (Web Page, 4 June 2018) <https://inclusivity.network/inclusivity-1-1-billion-people-without-official-identity-id/>.

[40] Merlin Martinson, 'Blockchain-based Self-Sovereign Identity as a Means of Aid in International Humanitarian Crises' *ResearchGate* (June 2018) <https://www.researchgate.net/publication/329017509_Blockchain-based_Self-Sovereign_Identity_as_a_means_of_aid_in_international_humanitarian_crises>.

[41] 'DLT-based Identification in the Humanitarian Sector', *Sovrin* (Web Page, 31 July 2019) <https://sovrin.org/dlt-based-identification-in-the-humanitarian-sector/>.

[42] Mark F N Franke, 'Refugees' Loss of Self-Determination in UNHCR Operations Through the Gaining of Identity in Blockchain Technology', *Taylor and Francis Online* (9 June 2019) <https://www.tandfonline.com/doi/abs/10.1080/21565503.2020.1748069>.

[43] Paula Berman, 'Digital Identity As a Basic Human Right', *Impakter* (10 April 2018) <https://impakter.com/digital-identity-basic-human-right/>.

standards needed to facilitate the scaling of digital identity projects beyond local populations, encompassing the applications of a blockchain-based SSI.[44]

From a business and commerce perspective, SSI is beneficial in several aspects.[45] First, the adoption of SSI-powered applications represents a streamlined and quick process. No data synchronisations are required for extended onboarding and users can start using the system immediately after receiving their digital identity credentials. Second, the interoperability of SSI means that credentials are stored on the blockchain, cross-applicable[46] and can be leveraged for different use cases. Third, the use of cryptography in the blockchain makes tampering near impossible. Finally, SSI implements privacy by design as personal identifiers never change hands. This can reduce data storage and compliance costs for businesses in relation to the General Data Protection Regulation ('GDPR') requirements and reduce the damage resulting from any data breaches.[47]

III Analysis

Having considered its numerous applications across government and private business, achieving a mutually acceptable level of trust, which is necessary to the realisation of SSI, requires a justification of its underlying legal and policy facets. Reviewing the centrality of a governance framework and regulatory compliance is central to the formation of broad consensus surrounding the widespread adoption of SSI.

A *Governance Framework*

From a governance perspective, SSI has been described as 'the Internet for Identity', as it is accessible to everyone, available for improvement by anyone and is not owned by any one actor. Consequently, a governance or 'trust' framework that sets forth a protocol for SSI and is mutually agreed upon by all stakeholders needs to be established. This provides the necessary basis to establish trust in the distributed ledger, being the technology instrumental to the realisation of

[44] Internetbar.org, 'Digital Identity: Helping Redefine Access to Justice' on World Justice Project (Working Session Summary, 1 May 2019) <https://worldjusticeproject.org/world-justice-forum-vi/digital-identity-helping-redefine-access-justice>.

[45] Jan Keil, 'Self-Sovereign Identity Systems: How Businesses Win From Letting Go of Customers' Data', *Hackernoon* (Blog Post, 5 September 2019) <https://hackernoon.com/self-sovereign-identity-systems-how-businesses-win-from-letting-go-of-customers-data-1v3fz31n0>.

[46] Usable across various blockchain technologies and providers.

[47] 'Personal Data Breach', *European Data Protection Supervisor* (Web Page, 2020) <https://edps.europa.eu/data-protection/our-role-supervisor/personal-data-breach_en>; Agata Slater, 'On Self-Sovereign Identity: What's the Business Value of SSI?', *Hackernoon* (Blog Post, 29 November 2019) <https://hackernoon.com/self-sovereign-identity-what-is-the-business-value-uq6l36wh>.

SSI, the suitability of which can be evaluated in accordance with the legal principles that underlie the rule of law.

It is contended that public-key technology forms both the origin of the problem and solution for digital identities. Notably, blockchain's use of cryptography provides confidentiality and integrity to a system and can be used to securely communicate with other identities. However, unlike in the technical framework, trust issues persist in the SSI policy framework, as nobody trusts the public-key infrastructures of their competitors. Indeed, different governments are supporting the development of different SSI solutions. Additionally, both businesses and institutions also have difficulties trusting users to be truthful. The SSI movement is experiencing an average annual growth of 35%; however, it is predicted that less than 10% of dedicated identity apps will use DLT by 2023.[48]

To foster the widespread adoption of SSI it is important to involve a diverse group of stakeholders in the creation and development of a TPF to facilitate the establishment of common best-practice policies, legal frameworks and the continuous monitoring of their proper implementation. A TPF represents a technological, social, business and legal governance structure for SSI and should seek to ensure alignment, interoperability and confidence in SSI as a digital identity solution.[49]

Attention should be directed towards the Sovrin Governance Framework ('SGF') that serves as Sovrin's legal foundation and global governance model for SSI. The SGF is presented as a preferable option to the competing Pan-Canadian Trust Framework, which has been seen as technology agnostic by comparison.[50] Further, the SGF defines the business, legal and technical policies for the Sovrin web of trust as a foundational layer upon which domain-specific governance frameworks can be built.[51] Finally, the contents of the SGF embody the 10 guiding principles of SSI and also encompass decentralisation by design, privacy by design, security by design and data protection by design.[52]

Sovrin is a decentralised identity system based on a distributed ledger and the leading organisation offering a DLT-based identity solution. Sovrin offers a publicly available,

[48] Tracy Molino, 'Practical Application of Distributed Ledger Technology: Self-Sovereign Identity on the Blockchain, *Dentons* (Web Page, 21 October 2019) <https://www.dentons.com/en/insights/articles/2019/october/21/practical-application-of-distributed-ledger-technology#_ftn10>.

[49] Culter et al (n 5) 10.

[50] Tim Bouma, 'Canada: Enabling Self-Sovereign Identity' *Medium* (Blog Post, 6 April 2020) <https://medium.com/@trbouma/canada-enabling-self-sovereign-identity-efcfda2aa044>.

[51] 'Sovrin Governance Framework', *Sovrin* (Web Page, 2020) <https://sovrin.org/library/sovrin-governance-framework/>.

[52] 'Sovrin Governance Framework V2 – Master Document V2', *Sovrin* (Web Page, 2020) <https://sovrin.org/wp-content/uploads/Sovrin-Governance-Framework-V2-Master-Document-V2.pdf>.

permissioned distributed ledger that allows public access to identity owners.[53,] Sovrin's identity as a universal trust framework is attributed to its use of decentralised identifiers ('DIDs') as a standard and interoperable format to represent individual's public digital presence. Further, verifiable claims allow standard and interoperable trustworthy assertions to be made about DIDs and the Sovrin ledger. This provides the means of discovering the keys and endpoints of a DID while recording information about the claims.[54] Sovrin has since evolved to govern the 'Sovrin Ecosystem' as a decentralised global network of networks interoperating in accordance with the TOIP stack.[55]

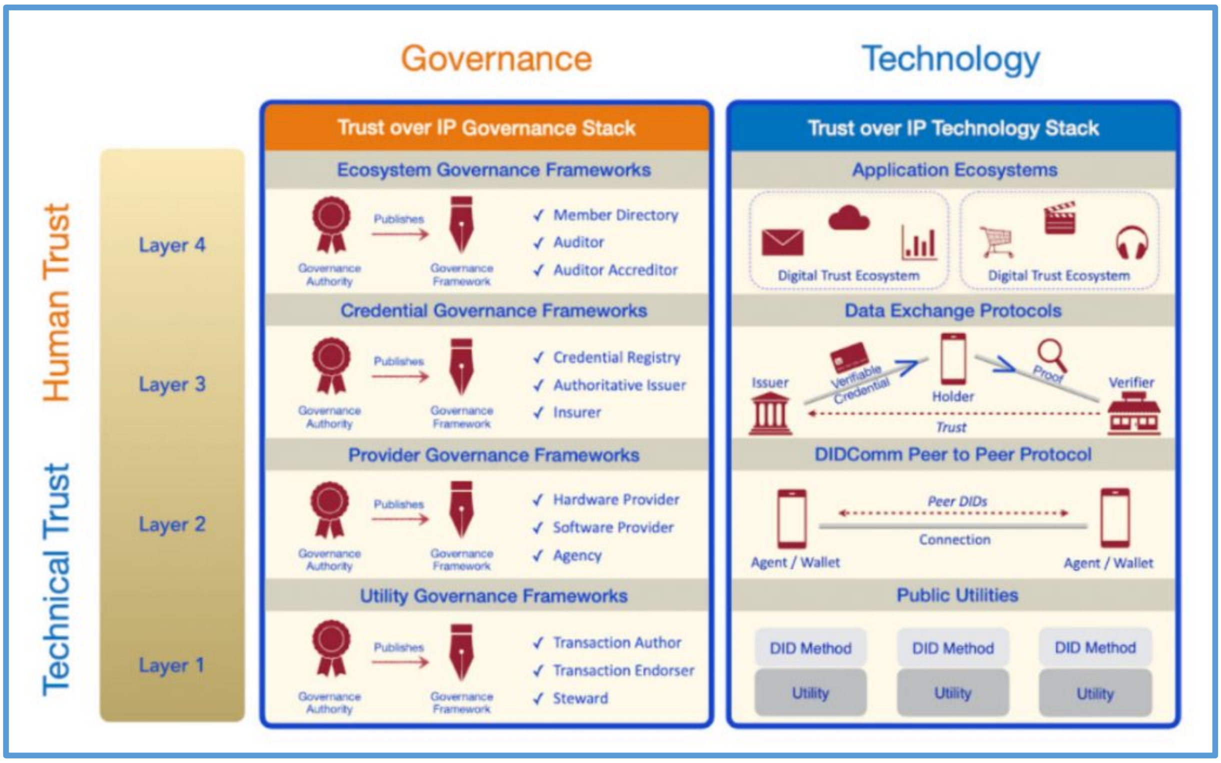
The TOIP foundation represents a new project aimed at enabling the trustworthy exchange and verification of data between parties over the internet. It seeks to provide a common standard that provides users with confidence in relation to the confidentiality, integrity and availability of their data. The TOIP stack represents a full architectural framework for digital trust that is based on the interaction between technology and governance.

[53] Nicky Morris, 'How Sovrin will Prevent Identity Leakages like Equifax' on Ledger Insights (Web Page, 15 September 2017) <https://www.ledgerinsights.com/sovrin-hyperledger-indy-Blockchain-identity-equifax/>; SSI Ambassador, 'The Growth Factors of Self-Sovereign Identity', *Medium* (Blog Post, 14 April 2020) <https://medium.com/@SSI_Ambassador/the-growth-factors-of-self-sovereign-identity-33aa3cc17ce7>.

[54] Phillip J Windley, 'Universal Trust Framework', *Medium* (Blog Post, 30 January 2017) <https://blog.sovrin.org/universal-trust-framework-5f37cfc65e35>.

[55] Alexander Andrade-Walz, 'Launching the Trust over IP Foundation and What it Means for Portable, Digital Identity', *Evernym* (Blog Post, 5 May 2020) <https://www.evernym.com/blog/trust-over-ip-foundation/>.

Figure 1. The TOIP Stack[56]



It is contended that the TOIP stack (see Figure 1) provides a blueprint for policy interoperability between institutions, as it is based om a common understanding of the functions of SSI and combines both technical and policy interoperability to create a complete digital trust architecture. As Figure 1 shows, the TOIP stack prioritises practical governance and policy considerations as the means of driving business, legal and social acceptance. Thus, it follows that TOIP-based solutions should interpret the stack from the bottom-up by considering business requirements, then policy requirements and finally, technology components. The governance appeal of the stack is that it incorporates privacy by design and thus satisfies the legal and regulatory compliance requirements set out in the GDPR, Canadian Personal Information Protection and Electronic Documents Act ('PIPEDA'), California Consumer Privacy Act ('CCPA') and the US Health Insurance Portability and Accountability Act ('HIPAA').[57]

Assessing the suitability of the TOIP stack as a definitive TFP solution, conducive to the widespread adoption of SSI by both governments and individuals, requires the establishment of the relationship between the legal principles that underlie the ROL and the technical features associated with the TOIP stack. The ROL is understood as an overarching principle that ensures that all groups and individuals within society are governed equally, justly and fairly by the law,

[56] Alexander Andrade-Walz, 'Launching the Trust over IP Foundation and What it Means for Portable, Digital Identity', *Evernym* (Blog Post, 5 May 2020) 18 <https://www.evernym.com/blog/trust-over-ip-foundation/>.
[57] 'FAQ', *Trust Over IP Foundation* (Web Page, 2020) <https://trustoverip.org/about/faq/>.

that the people should be ruled by the law and obey it and that the law should be such that people will be able and willing to be guided by it.[58] A non-exhaustive list of elements that comprise the ROL concept include:[59]

1. Access to justice and judicial review
2. Legal certainty
3. Proportionality
4. Equality and non-discrimination
5. Transparency.

The notion of access to justice has been associated with concerns over the independence of the judiciary, the independence and impartiality of judicial authorities and the effective implementation of judicial decisions. Consequently, legal certainty requires that citizens know in advance what the legal consequences of the law will be before committing to any course of action. Under economic law, legal certainty may bring about a reduction in transaction costs and increase the efficiency of business. Additionally, proportionality requires the balancing of risks against benefits to ensure that any action taken is proportional to its objectives and has been associated with the assessment of restrictions of fundamental human rights.[60] Further, equality and non-discrimination concern the prevention of discriminative actions that result in inequality; thus, any differences in treatment must strike a fair balance between protecting community and individual interests. Finally, transparency concerns the right of access to information, being conducive to promoting responsibility and accountability.

The evaluation of the SSI TIOP stack draws relevance from the following shared trust elements and governance traits that are present within the ROL: the decentralisation of authority and the separation of powers; the curbing of the discretionary powers granted to a centralised authority/intermediary in the interests of certainty and predictability; and the transparency evident within a blockchain's features as a public record keeping system.[61]

First, the TOIP stack provides the blueprint for policy interoperability between institutions. Specifically, the decentralisation of authority occurs via the use of blockchain

[58] 'Principles', *Australia's Magna Carta Institute* (Web Page, 2020) <https://www.ruleoflaw.org.au/principles/>.
[59] Rafael Leal-Arcas, 'Essential Elements of the Rule of Law Concept in the EU' *SSRN* (20 August 2014) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2483749>.
[60] Ibid 3–5.
[61] Denise Meyerson, 'The Rule of Law and the Separation of Powers' (2004) 4 *Macquarie Law Journal* 1, 1–6.

technology and the creation of an interdependent ecosystem within the Credential Trust Triangle ('CTT') between the issuers, verifiers and holders of digital identity credentials. The mutual trust shared between these three elements of the SSI ecosystem under the CTT relates to the notion of the separation of powers, which is crucial to addressing the trust gap and supporting the adoption of SSI.[62]

Second, the use of blockchain technology as a central aspect of SSI empowers individual digital identity holders over authorities via the use of public-key cryptography[63] and thus creates a secure and trusted identity framework that does not require the involvement of intermediaries as the holders and conveyors of trust. This occurs through the separation of the e-trust mechanism from the service of holding the record. It also eliminates the ability of the intermediary to exploit the powers afforded to it under traditional identity systems and promotes the principles of certainty and predictability that are central to the TPF.[64]

Third, the blockchain's features as a secure and trusted public record keeping system relates closely to the principles of transparency under the ROL. Drawing upon the history of trusted repositories of public records in Roman Law, the presence of transparency as a principle of ROL is established under the basis of trusted public record keeping. Under the Justinian code, an archive was defined as *locus publicus in quo instrumenta deponuntur* (the public place at which deeds are deposited), *quatenus incorrupta maneant* (so that they remain uncorrupted), *fidem faciant* (provide trustworthy evidence) and *perpetua rei memoria sit* (represent a continuing memory of that to which they attest).[65]

Blockchain's public-key cryptography system exists as a contemporary iteration of trusted public record keeping. It provides a novel means to balance the need for individual privacy against the need for transparency. Specifically, blockchain services protect user identities via strong and uncrackable cryptography, while also assigning each user a de-identified public address that is publicly viewable and allows anyone to view the holdings and transactions associated with any address.[66] This transparency enables consumers to hold the businesses they

[62] 'Learn About Trust Over IP', *IdRamp* (Web Page, 2020) <https://idramp.com/learn-about-trust-over-ip/>.

[63] Dan Gisolfi, 'Self-Sovereign Identity: Why Blockchain?', IBM (Blog Post, 13 June 2018) <https://www.ibm.com/blogs/Blockchain/2018/06/self-sovereign-identity-why-Blockchain/>.

[64] Philip J Windley, 'Sovrin Use Case: Healthcare', *Medium* (Blog Post, 14 November 2016) <https://blog.sovrin.org/sovrin-use-case-healthcare-69faca0f1437>.

[65] Victoria L Lemieux, 'Blockchain and Public Record Keeping: Of Temples, Prisons, and the (Re)Configuration of Power', *Frontiers* (21 July 2019) <https://www.frontiersin.org/articles/10.3389/fbloc.2019.00005/full>.

[66] Quantilus, 'How Blockchain Can Make Transactions More Transparent and Safe', *Quantilus* (Web Page, 24 October 2018) <https://quantilus.com/virtual-reality-future-2-2/>.

work with accountable for their spending, to track and boost supply chain cybersecurity and to counter fraudulent activities.

B *Regulatory Compliance*

Clarifying how a TPF for SSI can be established from a legal and compliance perspective is necessary to ensure its widespread adoption by business and government entities and support the creation of binding interactions and relationships within the digital identity ecosystem through defined rights and duties. It is acknowledged that there exists a significant trust gap across sections of the population who have little trust in their governments, who do not wish to be registered by authorities and who view the implementation of identity systems and technology as illegitimate violations of their right to privacy.[67]

Unlike many other public services, such as healthcare and education services, only large central governments have possessed the technical capacity, organisational capability and legal authority to effectively register people into public identity registries and issue identity documents to people based on their registration. Governments have served as the primary source of foundational identities. It should be noted that the term foundational identity refers to an identity that has been established or changed as a result of a foundational event (eg, a birth or a death).[68] However, large central governments operate at a cost, both in terms of the overhead processes associated with statecraft and in distorted incentives.[69]

Harmonising SSI with data and privacy law is necessary to address the trust gap, advance a robust TPF and promote SSI as a trusted digital identity solution. National SSI implementations, which have a high degree of government support, are more likely to get adopted. Using blockchain to implement legal processes, such as issuing and recording national identifications under SSI, may involve or demand changes to the law and the legal systems that interpret, create and implement such legal processes. Where SSI involves the storage or transmission of sensitive or private data, this raises the matter of compliance with international data privacy and security laws.[70] All participants on the distributed ledger can view all of the records forming part of the chain, but not their contents. However, the process of storing and

[67] Lee S Strickland and Laura E Hunt, 'Technology, Security, and Individual Privacy: New Tools, New Threats, and New Public Perceptions' (2005) 56(3) *Journal of the American Society for Information Science and Technology* 229.

[68] SSI Ambassador (n 53).

[69] Davidson et al (n 6) 642.

[70] 'Self-Sovereign Identity and Decentralised Identity: Control Your Data', *Dragonchain* (Web Page, 27 August 2019) <https://dragonchain.com/blog/decentralised-identity-self-sovereign-identity-explained/>.

transmitting personal data off ledger presents the same privacy risks inherent in the technology being used to store and transmit such off-ledger data. As blockchain expands into the realm of digital identity under SSI, it may cause tension with a number of privacy laws.[71]

1 *European Union*

In the European Union ('EU'), cross-border digital identities are an essential element to the common economic community. The GDPR and the electronic 'IDentification, Authentication and trust Services' ('eIDAS') regulations contain common legal requirements that aim to remove economic and organisational barriers between EU member states and incentivise citizens and companies to act more strongly within the European internal market.[72] However, policymakers must first overcome three key issues related to the GDPR and blockchain: 1) the anonymisation of personal data; 2) the identification of obligations of data controllers and processors; and 3) the exercise of some data subject to rights.[73]

First, the GDPR only applies to personal data. However, SSI involves four types of data: DIDs, credentials, revocation of credentials and hashes. This raises the question of whether a person could be identified with certain data using all the means likely to be used. The principles of data protection do not apply to anonymous information under art 4 of the GDPR. Under Recital 26 of the GDPR, to be considered personal data, the data needs to convey some information about the data subject.[74] Credentials and revocations are usually considered personal data; however, the application of GDPR protections to DIDs and hashes of personal data is more complex.

Where DIDs are created by data subjects, the subjects prove control of a DID by signing with a private key that is linked to the DID. A data subject cannot be identified unless a DID has been used once, after which the GDPR may be stated to apply automatically. Further, the classification of hashes of credentials or other objects as personal data is also considered on a

[71] Such laws include the CCPA, Singapore Personal Data Protection Act 2012 ('PDPA'), the Japan Act on Protection of Personal Information ('APPI'): see 'Self-Sovereign Identity and Decentralized Identity—Control Your Data', *Dragonchain* (Web Page, 27 August 2019) <*htt*ps://dragonchain.com/blog/decentralized-identity-self-sovereign-identity-explained; Culter et al (n 5) 7.

[72] Uwe Der et al, 'Self-Sovereign Identity—Opportunities and Challenges for the Digital Revolution', *arXiv* (5 December 2017) 2 <https://arxiv.org/abs/1712.01767>.

[73] Raffi Teperdjian, 'The Puzzle of Squaring Blockchain with the General Data Protection Regulation' (2020) 60(3) *Jurimetrics Journal* 24.

[74] 'Recital 26—EU GDPR', *Privazy Plan* (Web Page, 2020) <https://www.privacy-regulation.eu/en/recital-26-GDPR.htm>.

case-by-case basis. The context of the hash value must both identify with a data subject and convey additional information.[75]

Article 4(7) of the GDPR regulates the processing of personal data, imposing obligations and sanctions onto controllers and processors.[76] To determine who might be a controller it is necessary to be able to distinguish between data that are not stored on a blockchain and data that are stored on a blockchain. When a data subject is themselves considered a controller of the processing of their personal data, then the GDPR does not apply; however, it may still apply to processors whom process the data on behalf of the data subject.[77]

Article 17 of the GDPR outlines the right to be forgotten/erasure. This is a common problem for blockchain-based systems, as while off-chain data can be deleted easily, the deletion of on-chain data raises some difficulties. Notably, the right to be forgotten/erasure is not absolute and can only be exercised where a) the personal data is no longer necessary for its created purpose; b) the data is no longer held for a legitimate state interest; c) the data was processed unlawfully; or d) deletion is required for compliance with legal obligations.[78] Consequently, the issue is threefold: 1) a valid deletion request must be discerned; 2) that which constitutes personal data must be identified; and 3) the process for deleting the data must be defined.[79] When DIDs hashes of credentials or revocations are stored on a blockchain, a case-by-case analysis is required to determine if some data entries should still be considered personal data.[80] Clarifying the legal standards surrounding these steps will help contribute to the TPF for SSI.

Second, as the EU's main electronic identification trust framework for secure and seamless electronic interactions,[81] the eIDAS has a strong influence in the international regulatory space.[82] The goal of mutual recognition by EU states of electronic identification is to enable cross-border interactions by EU citizens using their own national eIDentification ('eID'). This mutual recognition is ensured by the eIDAS interoperability framework and is based on the deployment of national eIDAS nodes managing the cross-border exchange of information.The integration of

[75] Galia Kondova and Jorn Erbguth, 'Self-Sovereign Identity on Public Blockchains and the GDPR', *SSRN* (30 January 2020) 344 <https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3515213>.
[76] 'GDPR Article 4—Definitions', *IT IP Law* (Web Page, 2020) <https://www.gdpr-expert.com/article.html?mid=7&id=4#textesofficiels>.
[77] Kondova and Erbguth (n 75) 344.
[78] Culter et al (n 5) 8.
[79] Arjun Govind, 'Is Self-Sovereign Identity the Answer to GDPR Compliance?' *R3* (Blog Post, 20 April 2020) <https://www.r3.com/blog/is-self-sovereign-identity-the-answer-to-gdpr-compliance/>.
[80] Kondova and Erbguth (n 75) 345.
[81] Craig Wright, 'Digital Signature Rules and their Relationship to Bitcoin' *Medium* (Web Page, 16 October 2018) <https://medium.com/@craig_10243/digital-signature-rules-and-their-relationship-to-bitcoin-b1faeae1f446>.
[82] The Regulation (EU) N°910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation).

eIDAS guidelines demonstrates an inter-governmental TPF that provides a viable means of adopting and enacting SSI, under which both SSI systems and governmental eID systems are highly complementary and mutually enforcing.[83]

Finally, there is ongoing work under the European Self-Sovereign Identity Framework ('ESSIF') to deliver EU-wide cross-border public services using blockchain technology.[84] The ESSIF aims to implement a generic SSI capability, which should allow users to create and control their own identity across borders without relying on centralised authorities and improve institutional efficiency.[85] As the project is still in progress, a number of legal questions concerning the TPF level of assurances, governance aspects and conformity have yet to be decided.[86]

2 *Australia*

In Australia, the lack of direction surrounding the adoption of SSI has been succeeded by the release of the government's 2020 National Blockchain Roadmap.[87] The federal government views de-identification and the use of pseudonyms as insufficient measures in protecting the privacy of blockchain users and in complying with the *Privacy Act 1988* (Cth) ('the *Privacy Act*'), under which the mere risk of a link forming between the data subject and the blockchain identifiers could result in a potential data breach.[88] Further, the decentralised nature of the blockchain means that there is often no responsible party to seek remedy for privacy breaches or any ways to remove PII from the ledger.[89]

A blockchain-based SSI system provides a viable digital identity solution for Australia; however, its widespread adoption would be contingent upon compliance with data and privacy protections under the Australian Privacy Principles ('APP'). The APP applies to any organisation

[83] Culter et al (n 5) 11; Carlos Gomez Munoz, 'eIDAS Supported SSI' *European Commission* (Web Page, 2019) <https://ec.europa.eu/futurium/en/eidas-observatory/ssi-and-eidas-vision-how-they-are-connected-share-your-views>.

[84]'European Self Sovereign Identity Framework Laboratory' *CORDIS* (Web Page, 1 November 2019) <https://cordis.europa.eu/project/id/871932>.

[85] SSI Ambassador, 'eSSIF: The European Self-Sovereign Identity Framework' *Medium* (Web Page, 3 February 2020) <https://medium.com/@SSI_Ambassador/essif-the-european-self-sovereign-identity-framework-4572f6875e12>.

[86] Alex Preukschat, 'eIDAS Regulation: Anchoring Trust in Self-Sovereign Identity Systems—Ignacio Alamillo—Webinar 49' *Simeetup* (Web Page, 29 February 2020) <https://ssimeetup.org/eidas-regulation-anchoring-trust-self-sovereign-identity-systems-ignacio-alamillo-webinar-49/>.

[87] Department of Industry, Science, Energy and Resources, 'National Blockchain Roadmap' *Australian Government* (Web Page, February 2020) <https://www.industry.gov.au/data-and-publications/national-Blockchain-roadmap>.

[88] *Privacy Act 1988* (Cth) ('the *Privacy Act*').

[89] Ibid, 16.

or agency covered under the *Privacy Act* in respect of personal information. The 13 principles covered under the APP govern standards, rights and obligations around:[90]

- The collection, use and disclosure of personal information.
- An organisation or agency's governance and accountability.
- The integrity and correction of personal information.
- The rights of individuals to access their personal information.

Individuals have the right to be informed what kind of information is being collected about them. Specifically, individuals have the right to 1) be informed of how such information is being collected; 2) understand why their personal data are being collected; 3) access their personal information for review or correction; 4) be informed of any data breach that affects them; and 5) have their data stored securely and protected from misuse.[91]

The APP represents principles-based law. It provides organisations with the flexibility to tailor their personal information handling practices to their business models and individual needs. A breach of an APP represents an 'interference with the privacy of an individual' and may lead to regulatory action and penalties.[92] In relation to the privacy principles, APP 11 requires that APP entities take 'reasonable steps' to protect personal information from misuse, interference and loss and from unauthorised access, modification or disclosure (i.e., data breaches). SSI reduces the costs and risks associated with information protection, which is important for an APP entity complying with its requirements under APP 11. Where an APP entity must have adequate cybersecurity measures in place to protect all personal information it holds or is responsible for, SSI reduces the associated costs and risks by removing the need for a single entity to store personal data through both its decentralised nature. The APP boosts the network security via the use of a zero-knowledge proof ('ZKP') encryption scheme.[93]

SSI may be viewed as a process that adheres to the requirements of the APP. It embodies privacy by design via its use of ZKP schemes that enable people to access control, delegate and

[90] Office of the Australian Information Commissioner, 'Australian Privacy Principles' *Australian Government* (Web Page, 2020) <https://www.oaic.gov.au/privacy/australian-privacy-principles/>.
[91] Sonia Hickey and Ugur Nedim, 'Australia: Australian Privacy Laws Must Be Strengthened' *Mondaq* (Web Page, 6 February 2020) <https://www.mondaq.com/australia/data-protection/890930/australian-privacy-laws-must-be-strengthened>.
[92] Ibid.
[93] Alec Christie and James Wong, 'Comparative Guides—Cyber Security' *Mondaq* (Web Page, 2020) <https://mondaq.com/Guides/Results/16?country=13&thechapter=1,2,3,4,5,6,7&question=1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23>.

consent to their PII by sharing only revenant data.[94] ZKP schemes use cryptography to prove a statement from Party A (prover) to Party B (verifier) without revealing anything else. ZKP schemes require several properties to be usable: completeness, soundness and zero-knowledgeness. Entities on an SSI network can issue credentials that identity holders keep in their digital wallet. Pieces of personal information in relation that credential (eg, an address or a social security number) are called 'attributes' and ZKP schemes are created using these attributes. Thus, identity holders can create ZKP schemes to prove aspects of their attributes, including equality, inequality and set membership.[95]

Further, the existing definition as to what constitutes 'personal information' has been adversely affected by the decision of the Full Court of the Federal Court of Australia in relation to metadata in *Privacy Commissioner v Telstra Corporation Limited.*[96] The Court held that data is only 'personal information' if a person is the actual subject matter of that information; thus, 'personal information' may not include data that only reveals a person's identity if it is linked with other data.[97] Accordingly, the public nature of transactions on the blockchain and the ability to infer the identity behind the de-identified public address through the analysis of transactions and interactions with real-world services means that the adoption of SSI and blockchain is not immune to the issue of data linking/data matching (ie, the comparison of multiple systems of records to aggregate data about an already identified subject).[98] To create the ideal regulatory and legal basis for the adoption of a blockchain-based SSI system as a digital identity solution, the government must broaden its definition of personal information to encompass metadata.

It is foreseeable that the viability of SSI as a digital identity solution in Australia will encounter similar legal issues to those observed under the GDPR. Specifically, harmonising the technology with Australia's data protection laws will require a consideration of the legal requirements of APP 3–5 in relation to the collection, handling and notification of personal

[94] Warick Ashford, 'Self-Sovereign ID Key to Data Privacy' *Computer Weekly* (16 May 2019) <https://www.computerweekly.com/news/252463475/Self-sovereign-ID-key-to-data-privacy>.

[95] Mike Lodder, 'The Sovrin Network and Zero Knowledge Proofs' *Sovrin* (Web Page, 3 October 2018) <https://sovrin.org/the-sovrin-network-and-zero-knowledge-proofs/>.

[96] *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4; Karliana Reid, 'Law and Tech during COVID-19: Is the Government's Proposed New App our Saving Grace or a Potential Privacy Issue?' *VSCL* (Web Page, 17 April 2020) <https://www.vscl.org.au/law-and-tech-during-covid-19/>.

[97] Jake Goldenfein, 'Australia's Privacy Laws Gutted in Court Ruling on What is "Personal information"' *The Conversation* (19 January 2019) <https://theconversation.com/australias-privacy-laws-gutted-in-court-ruling-on-what-is-personal-information-71486>.

[98] Alberto Cuesta Cañada, 'Privacy or Truth?' *Medium* (Web Page, 13 May 2019) <https://medium.com/hackernoon/privacy-or-truth-f09b92ae6ffb>.

information, APP 8 in relation to the cross-border disclosure of personal information and APP 12 in relation to access to personal information.[99]

IV Conclusion

The growing prominence of SSI as a digital identity solution across the commercial and humanitarian sectors requires consensus and cooperation in the creation of a TPF. The adoption of SSI for the management of identity data has been shown to provide numerous benefits, including increased control over one's identity, increased privacy and increased security. Additionally, businesses that have a vested interest or statutory obligation will be able to reduce the time and money they spend verifying people's identities. However, where governments serve as the primary source of foundational identities, the issuer of foundational identity documents[100] and the preliminary trust anchors for SSI, the national or widespread adoption of SSI as a digital identity solution requires consensus surrounding the governance and compliance facets of the TPF for SSI. The emerging consensus surrounding SSI necessitates the codification of the 10 guiding principles of SSI. For SSI and DLT to drive change, true and meaningful progress requires technology-enabled change of the status quo within law and policy rather than the mere and value-neutral digitisation of existing paradigms and power structures.[101]

Further, unanimity surrounding SSI requires the development of a trust/governance framework that underlies SSI. This calls for the adoption of the TOIP stack as a blueprint for policy interoperability between institutions that is based upon a common understanding of the functions of SSI. This must be supported by policies that emphasise the relationship between the TOIP stack and principles of the ROL. Any such policies should reference the decentralisation of authority, the elimination of third-party intermediaries and state that the public record keeping system of blockchain is commensurate to the separation of powers,

[99] Office of the Australian Information Commissioner, 'Australian Privacy Principles Quick Reference' *Australian Government* (Web Page, 2020) <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-quick-reference/>.

[100] Primary source of foundational identities may overlap with the issuer of foundational identities. Conversely, they may be distinguished where the primary source is concerned solely with maintaining identity records and corroborating identity requests and the issuer is concerned solely with the collection of biometrics in forming new identity documents.

[101] A. Grinbaum and C. Groves, 'What is 'Responsible' about Responsible Innovation? Understanding the Ethical Issues' in Richard Owen, John Bessant and Maggy Heintz (eds) *Responsible Innovation: Managing the Responsible Emergence of Science and Innovation in Society* (Wiley and Sons, 2013) 119; Oskar J. Gstrein and Dimitry Kochenov, 'Digital Identity and Distributed Ledger Technology: Paving the Way to a Neo-Feudal Brave New World?' *Frontiers in Blockchain* (Web Page, 12 March 2020) <https://www.frontiersin.org/articles/10.3389/fbloc.2020.00010/full>.

certainty, predictability and transparency. Thus, the SGF must be adopted as the foundational layer upon which domain-specific[102] governance frameworks can be built.

Finally, legal certainty concerning SSI requires consideration of how associated data and privacy laws will affect the development of a TPF for SSI. Further, consideration must be given to the need to devise new laws that reconceptualise the definition of privacy as it relates to blockchain technologies. The EU's GDPR can be used to gain an understanding of how countries lacking coherent data protection laws can adjust to support the adoption of SSI digital identity solutions by granting data subjects' control over their PII.[103] Consequently, the Australian government must also address its policy and legal shortfalls in relation to privacy protections for metadata to preclude the potential adverse effects that the data linking of PII may have on the viability of SSI as a digital identity solution.

It is recognised that the adoption of blockchain-based SSI has significant operational benefits for businesses and governments alike. These benefits may take some time to be fully realised; however, the empowering of individual digital identity holders through SSI and its broad applications to reduce risks and boost cyber resilience makes the adoption of SSI an inevitability.

[102] Considering alternative digital identity frameworks or domains which may exist or be proposed.
[103] Alastair Berg et al, 'Some Economic Consequences of the GDPR' (2019) 39(2) *Economics Bulletin* 785, 785.