Self Sovereign Identity:

Data Owner Perspectives

July 2020

Octopus.sh

Self Sovereign Identity: Data Owner Perspectives

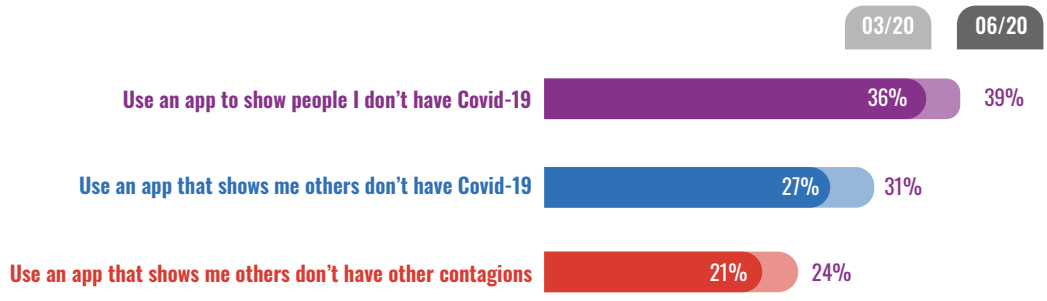
This year we've seen global governments and organisations using citizens' identity and their other personally identifiable information (PII) to help combat the global Covid-19 crisis. Many have launched aggressive (in some cases, forced) subscription campaigns for mobile contact tracing and test result sharing programmes.

In the process, the debate about protecting public safety vs protecting personal privacy is back at the forefront: how do we combat the contagious threat whilst preserving citizens' sovereignty over their digital identity, data security and personal anonymity?

But even before the Covid-19 pandemic escalated, more citizens were gaining greater control over more of their medical-related information. And as a new labor-market crisis emerges, citizens are also seeking sovereignty over their employment identity and PII.

This research report reveals compelling data owner self sovereign identity (SII) insights including:

- A significant percentage of US and UK citizens want sovereignty over their identity documentation and PII now
- SSI features important to citizens include secure PII storage and management, real-time visibility of PII sharing, revocation, multi-identity personas, verified attestations, identity sharing minimisation, such as zero proofs and connecting anonymously
- Citizens want control over application PII as an employment crisis escalates
- Covid-19-related medical PII sharing has increased in importance to citizens this year



As citizen's demand for PII sovereignty grows, Enterprise has a unique opportunity to leverage the innovative SSI technology to compliantly enhance trust with all stakeholders, gain competitive advantage, and improve customer NPV - whilst reducing PII storage costs and regulatory risk.

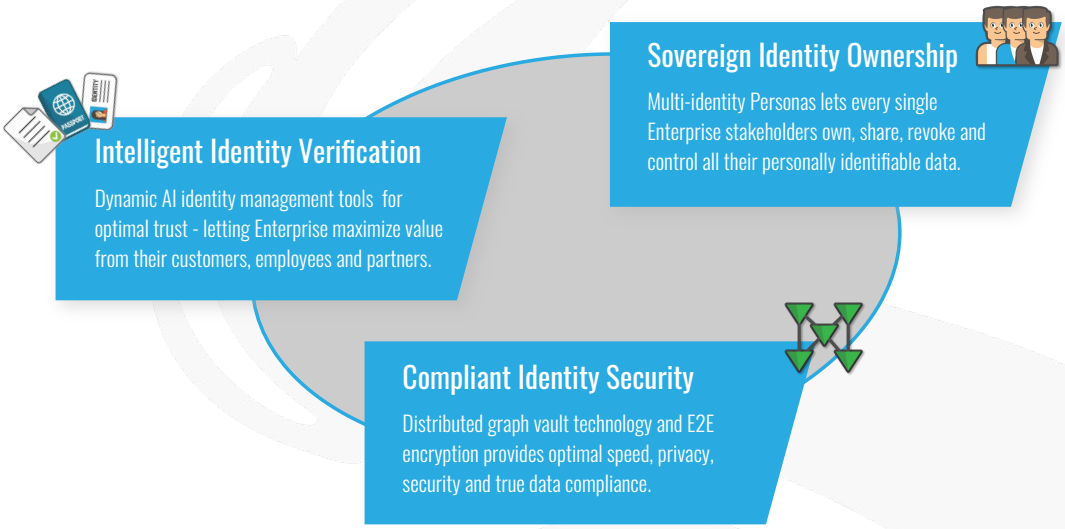
True Self-Sovereign Identity

SSI gives citizens complete control and ownership of all their personally identifiable information. It lets them share only the necessary data for interactions, transactions and communication with other entities.

Because SSI offers real-time identity updates and verification, Enterprise can leverage (consented-for) PII insights to increase cross-sell and upsell - and to better service customers, employees and partners. SSI built compliantly with properly decentralised technology and user-friendly features are attractive to organisations that want to avoid the high data storage costs and regulatory risk commonly found in centralised, federated and distributed ledger identity management systems. An enterprise that returns PPI to rightful-owning stakeholders sends a strong, positive message about trust to everyone associated with the organisation.

Meanwhile, SSI lets each user securely create, store, manage, share, track, revoke and own all their PII. They can easily reuse verified identity and attestations, giving them access to more private and public digital services. They can segment relationship groups into multi-identity communities whilst keeping track of all their PII in real time. Zero-knowledge proofs and identity field-level sharing minimises the amount of personally identifiable data needed for verification - increasing their trust in the overall identity verification process.

The leading end-to-end SSI solutions offer innovative and value-generating identity ownership, verification and data compliance capabilities:



Sovereign Identity Ownership

SSI ownership centers on citizens having complete authority and control of their identity - and user-friendly, highly-functional capabilities are required to facilitate this. Rather than basic mobile app capabilities, such as those found in many digital identity wallets, leading SSI solutions provide users with robust, feature-rich and fully-encrypted functionality and services.

All identity, qualifications, references, certifications, memberships, entitlements, attestations and other PII is stored, managed, shared and owned in hub-centric decentralised graph technology, such as distributed vaults. Citizens can use private and public community settings, multi-identity personas for sharing identity within segmented relationship groups, role-based connectivity, group messaging, activity stream feeds and real-time communication. All PII can be created and shared on a field level - including government-issued identity cards, certification documents or entirely new artefacts created by the citizen. These artefacts can be grouped into a single artefact for PII-intensive sharing activities, such as applying for a mortgage or signing up with a doctor. Private self-provisioning is completely anonymous with users never needing to share any PII with other middlemen - including the SSI solution provider - at any stage of onboarding.

Intelligent Identity Verification

Organisations considering new identity management solutions require innovative technology that compliantly captures essential characteristics of each stakeholders' identity. They need a trusted collection of personality cultural and historical characteristics, third-party identifiers and legally confirmed attributes to prove in real-time who each individual is throughout the lifetime of the relationship.

SSI let organisations securely authorise, authenticate and verify all types of users for all types of data transactions. It lets them manage decentralised user identities, their preferences, and profiles across multiple digital channels and devices. Both the organisation and the citizen can verify, store and manage trusted 3rd party attestations, such as biometric corroborated documents, a 3rd party credit header verification or a digitally-signed certifications from a lawyer.

Top solutions allow Enterprise to leverage out-of-bound biometrics for continuous authentication and use reputation-centric conferred trust scoring - which evaluates each user's credibility based on historical private and public network activity and behaviour. All the while zero-knowledge proofs and single-field sharing ensures only essential PII is used for citizen identification.

Compliant Identity Security

Leading SSI solutions are built following core privacy by design principles - offering adaptive, secure and controlled access to stakeholder identity and PII. They are compliant to global privacy regulation (e.g. GDPR, CCPA) providing true data ownership - including real-time consent and subject access request, revocation and the right to be forgotten. They must also offer real-time view of all data transaction history & audit - down to the field level.

Some top solutions have built-in Data Protection Office capabilities using multi-identity personas for compliance roles and rights management. And the most flexible, distributed technology enable identity transferability and portability allow all types and formats can be stored, managed and shared by citizens across multiple different platforms - whilst ensuring personal rights and freedoms are always protected.

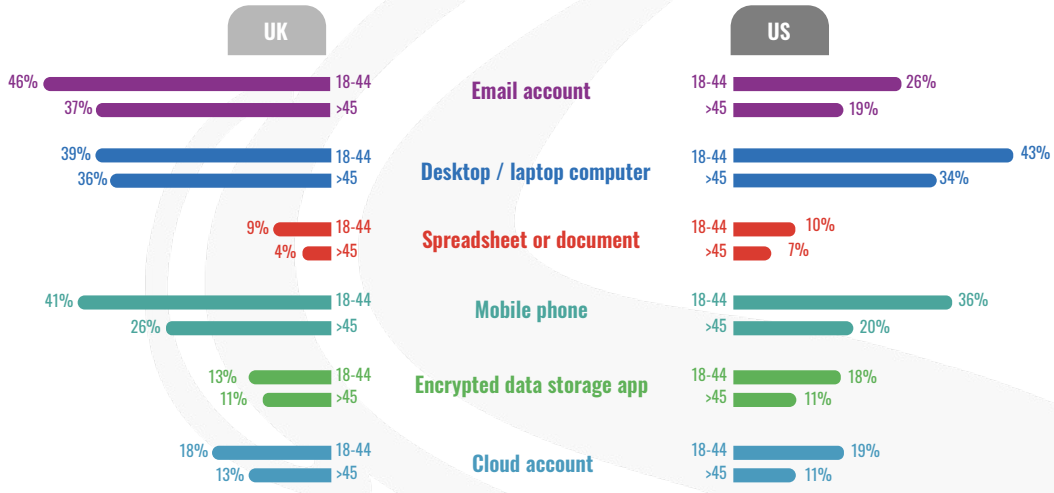
PII Ownership Perspectives in the UK and US

This research provides a view of 1000 American and British citizens' digital identity activity, preferences and receptivity to SSI features including:

- Current digital identity management
- Digital identity document sharing
- Stored verified identity types
- Digital identity security concerns
- Trust in 3rd party organisations to manage identity on their behalf
- Receptivity to mobile SSI features

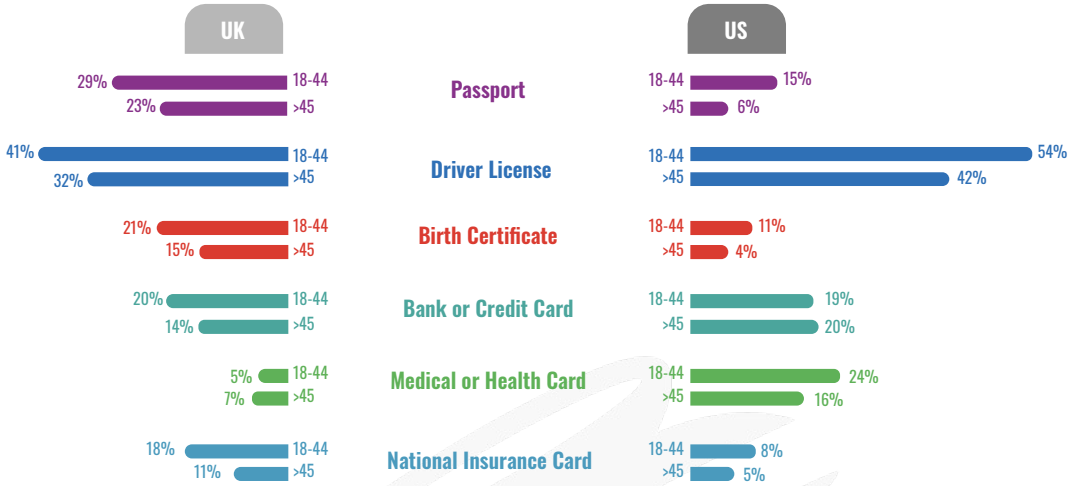
Current Digital Identity Management

When examining current digital identity management channels and mechanisms, we see that British citizens are most using email accounts and desktops. American are less likely to use email. There's a high use of mobile phones by the 18-44 segment in both countries. Overall, over 45s manage identity digitally less than the younger segment - although we see citizens in each age segment using encrypted PII storage apps, such as data and password managers and identity wallets.



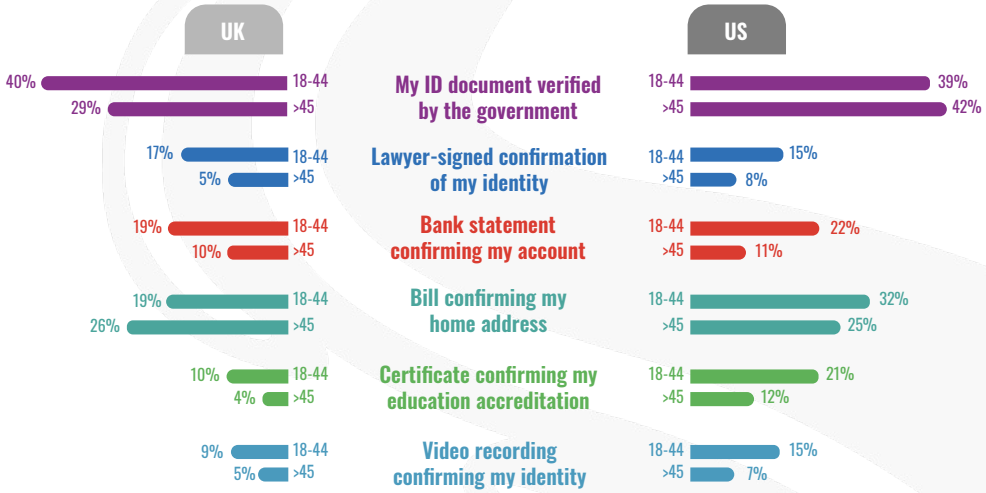
Digital Identity Document Sharing

Americans are more receptive to sharing their identity documents than British. But Americans appear less at ease with sharing a digital passport or birth certificate - although some (notably 18-45s) are comfortable sharing their digital driver's license. Although more British will share digital passports, they're not as keen on sharing medical health cards - which is less an issue for Americans.



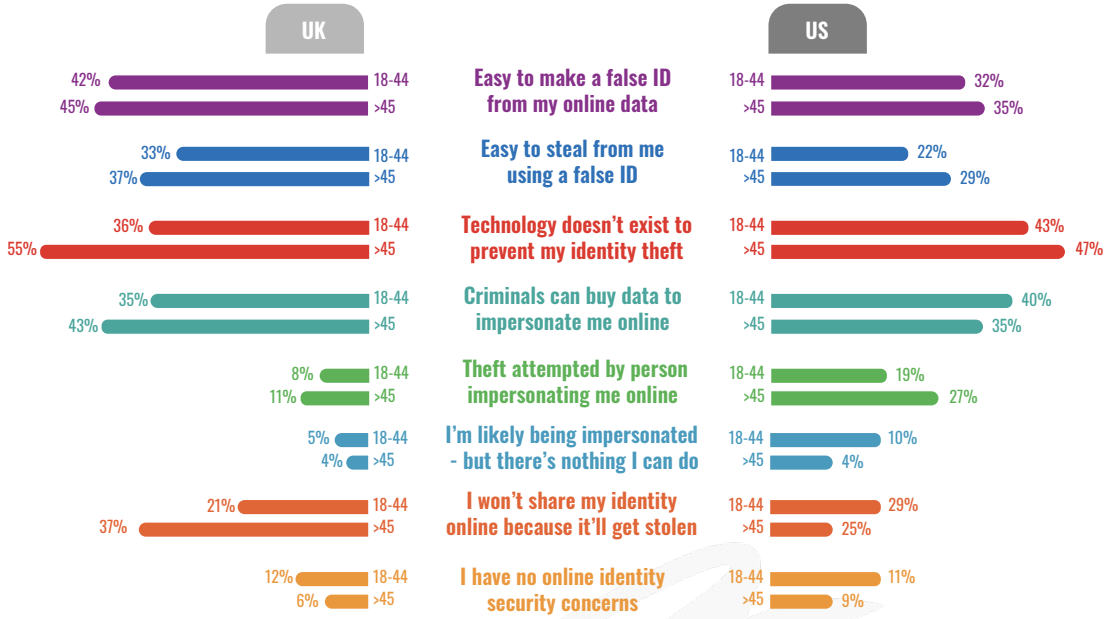
Stored Verified Identity Types

Both UK and US citizens show interest in storing confirmed identity attestations in a mobile app - notably a passport or driving license that has been verified by the government.



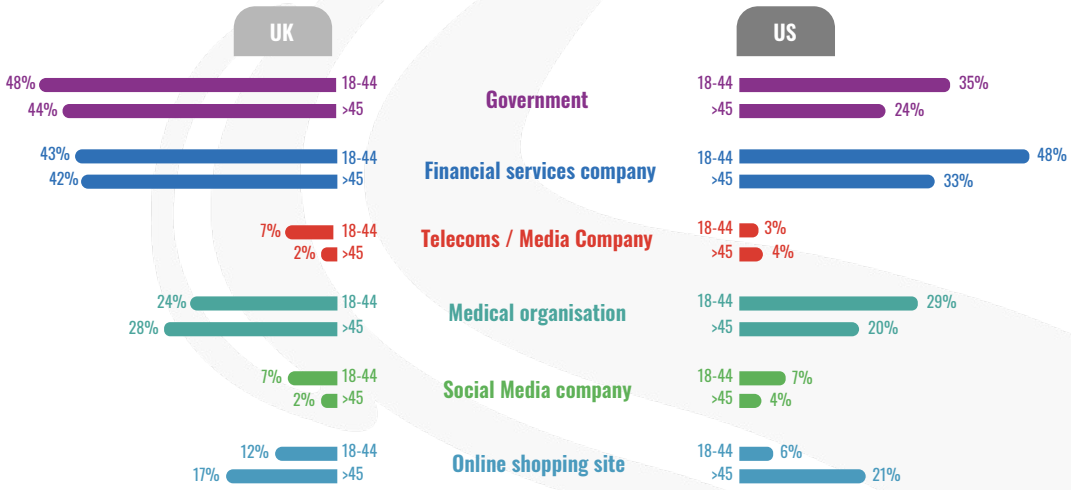
Digital Identity Security Concerns

Both US and UK citizens are concerned about their identity being hacked and used online. Over 41% believe criminals can buy their PII to impersonate them online - whilst 47% feel there's no adequate technology available to stop identity theft. Less than 10% have no digital identity security concerns.



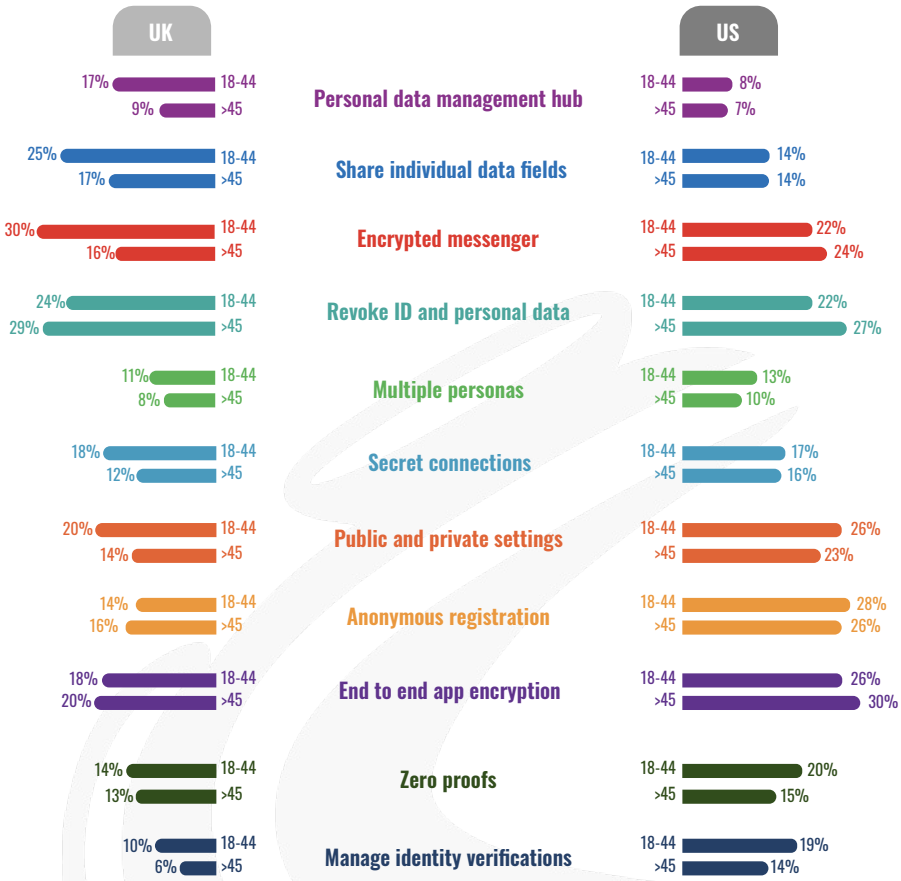
Trust in 3rd Parties for Digital Identity Management

The government is trusted more than financial institutions to manage users identity on their behalf in the UK, the opposite in the US - with little trust in Telecoms, Media or Social organisations.



SSI Application Feature Receptivity

Security and privacy SSI features are important to both British and Americans for managing and sharing digital identity and PII. Americans are particularly interested in end-to-end encryption and an anonymous registration that ensures no PII is revealed during the onboarding process. There is some interest in both countries for having both public and private settings for sharing PII. British 18-44 year olds show interest in encrypted activity exchange and messaging tools for sharing identity artefacts and other PII. More than ¼ of citizens surveyed want the ability to revoke their PII.



Covid-19 and Medical Health PII Ownership in US

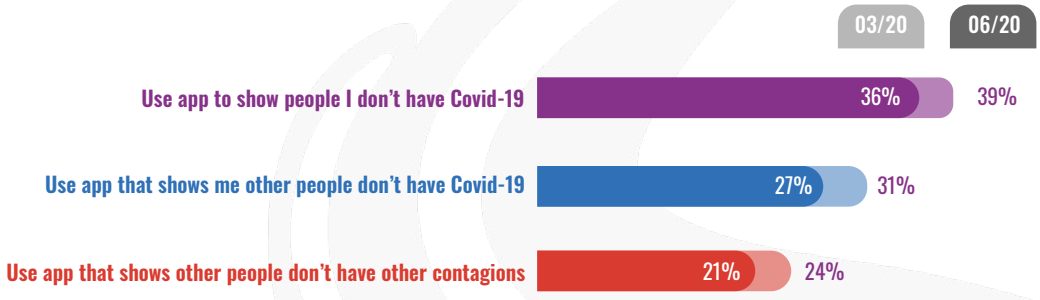
During the Covid-19 crisis, many global governments and other organisations have exercised emergency powers to access, analyse and make use of citizens' PII. In Taiwan, phone GPS triangulation is used by the police to ensure self-isolating people remain in their homes. In China, a mobile app green QR code confirms people have tested negative for the virus during random street checks. In the UK, the National Health Service is developing a heat-mapping surveillance app that traces people's location to help identify virus hotspots. And in the US, the Centre for Disease Control and Prevention have the power to not only force citizens into quarantine, but also access their identity and other PII on personal phones, devices, email and their homes.

Encouragingly, new European Commission guidance outlines that member nations building contact-tracing smartphone apps should use notifications and bluetooth technology — and no PII — to help fight the spread of COVID-19.

Research feedback from over 500 Americans suggests we may be entering an age when authorities, organisations and normal everyday people request real time medical health data from others - before sharing public and private areas such as workplaces, transport, restaurants and social events.

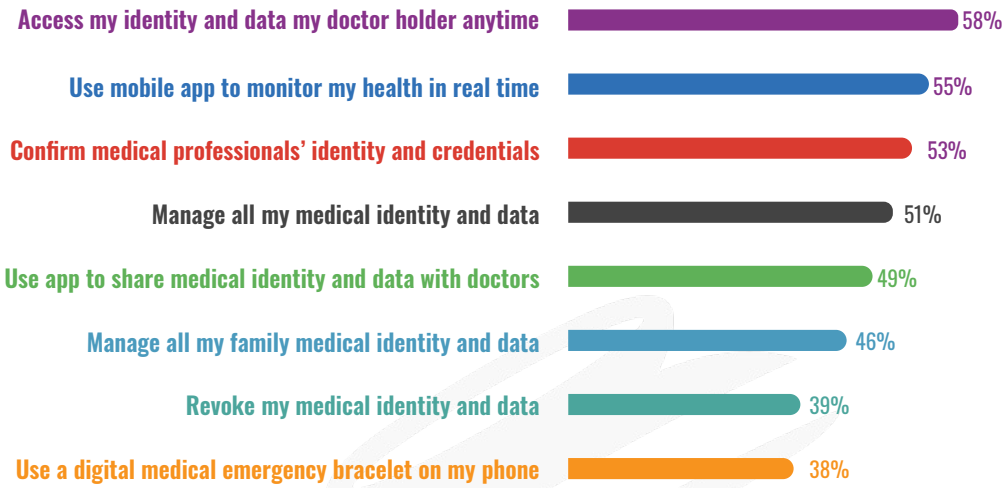
Covid-19 Test Result Sharing

Over a three-month period we've seen more Americans wanting more Covid-19 test-result sharing. Interestingly, more want to prove to others that they're negative versus demanding others prove to them they don't carry the coronavirus. Further analysis in 2020 will reveal whether this trend will continue - and how it's related to moral care for human life, job protection, online social reputation preservation and other factors.



Digital Health Identity and PII Management

Our research reveals that US demand for owning and sharing medical and health PII is significant - and shows that citizens want self sovereign control to manage it themselves. They most want real-time access to shared medical information, private health data tracking and management of all identity, prescriptions and other medical PII on mobile devices. Online identity and credentials checks to ensure medical professionals are who they say they are is also desired. Only 11% of those surveyed aren't interested in any digital medical health PII activities.



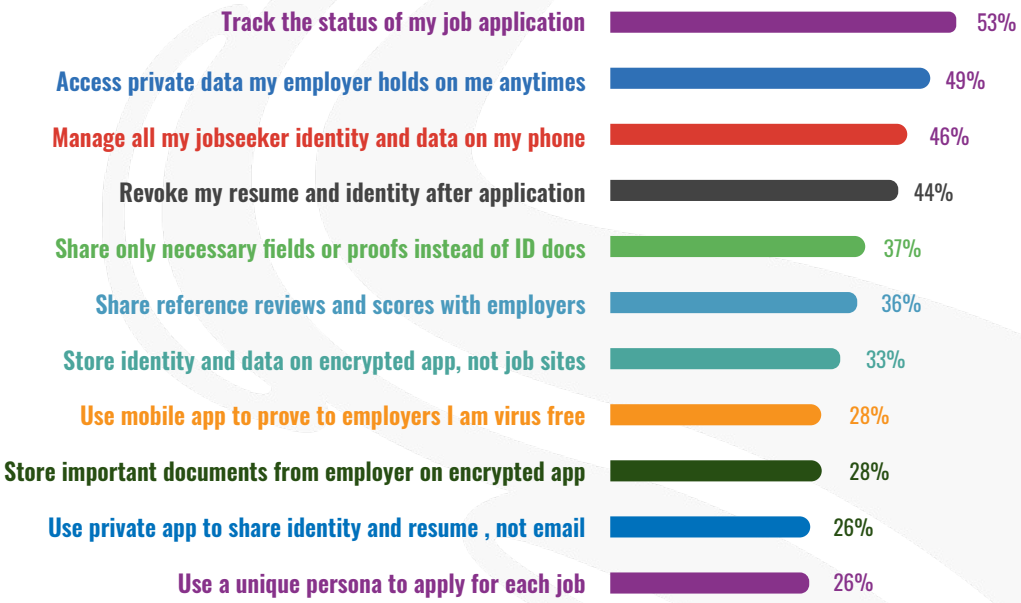
Digital Employment PII Ownership in US

The Covid-19 crisis is having both a medical and economic impact - most notably the surge in global unemployment. As more people try to re-enter the labour market, there is a greater importance on having compliant identity solutions for role applications. By effectively using candidate lifecycle management, attestation and referencing, project analysis and templating features, Enterprise can increase the volume and quality of candidates which will reduce attrition rates. Employers can request individual fields of personal data (zero-proofs) per role application and let applicants share and revoke PII artefacts, such as resumes, medical details, certifications, identity, references and attestations - as well as signed contracts, digital work passes and passwords after being employed.

The top SSI solutions offering identity personas let jobseekers personalise each application, allowing them to highlight strengths and experience - and be who they want to be for that particular role. Built-in data protection roles let employers instantly return PII to jobseekers at each point of the process - submission, shortlisting, interview, hiring and role termination. This allows employers to shortlist candidates without ever touching their PII - offering consent and right to be forgotten.

Digital Employment PII and Identity Management

Our research of over 500 Americans reveals interest in SSI and PII sharing. They want to manage their own jobseeker artefacts and have real-time visibility of their application status. More than a third want self-sovereign employment tools offering conferred trust scoring, zero-proof or field-level data sharing. And when citizens are in a role, nearly one half want access to the PII employers hold on them.



About Octopus.sh

Octopus.sh lets Enterprise focus on the value identity brings beyond verified access. Reduce identity management costs. Give customers their identity ownership back. Empower employees. Build trust with every single stakeholder.

- True self-sovereign identity: authorise, authenticate and verify everyone in real time
- Artefacts® Exchange Hub: feature-rich app securing every identity owner's social privacy
- Personas®: multi-identities for sharing identity, zero-knowledge proofs and attestations
- Intelligent Agents: autonomous and defensive protecting users from threats online
- Data Privacy: regulatory compliance with built-in DPO roles and rights

Our VaultChain® platform is built from distributed graph technology. It's what guarantees privacy, anonymity and security – ensuring no unauthorised access to any user data, ever. And it solves blockchain scalability, compliance and speed limitations – whilst offering data compliance for all organisations.

With Octopus.sh, it's a million vaults for a million customers – not one database holding a million customer records.

Intelligent identity. Intelligent privacy.

Contact:
Thomas John Behe
tj@octopus.sh
octopus.sh