Octopus.sh
Intelligent Privacy™

OIX OPEN IDENTITY EXCHANGE Member Whitepaper

Identity Credential and Personal Data Ownership Perspectives

Thomas John Behe

November 2020

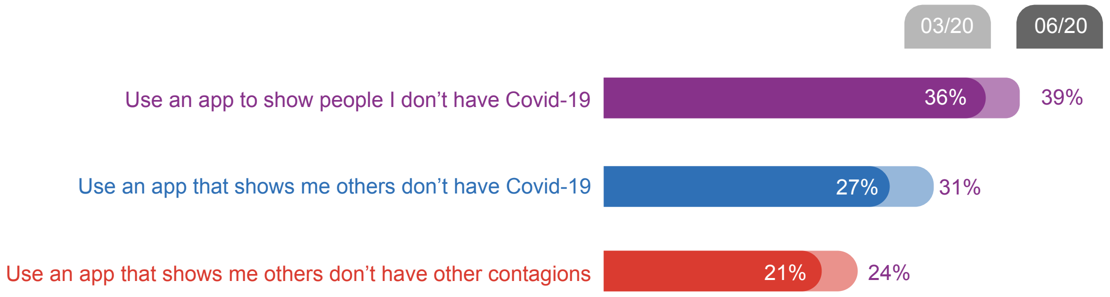
Identity Credential and Personal Data Ownership Perspectives

Many global organisations are using their citizens' identity and their other personally identifiable information (PII) to help combat the global Covid-19 crisis. Some have introduced aggressive (in some cases, forced) subscription campaigns for mobile contact tracing and test result sharing programmes. In the process, it's reignited the debate around protecting public safety vs protecting privacy: how to combat the contagious threat whilst preserving citizens' digital identity, security and anonymity?

But even before the pandemic hit, more citizens wanted more control and ownership of their medical information. And now as a new labor-market crisis emerges, citizens are also seeking sovereignty over their employment PII.

This research report offers new self sovereign identity (SII) insights including:

- UK & US citizens desire to own identity includes ID documentation and all PII
- Important features for UK and US 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
- US citizens want control over job PII as an employment crisis escalates
- Covid-19-related medical PII sharing has become more important to US citizens



Citizen's demand for SSI is growing. Enterprise has a unique opportunity to leverage the most 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.

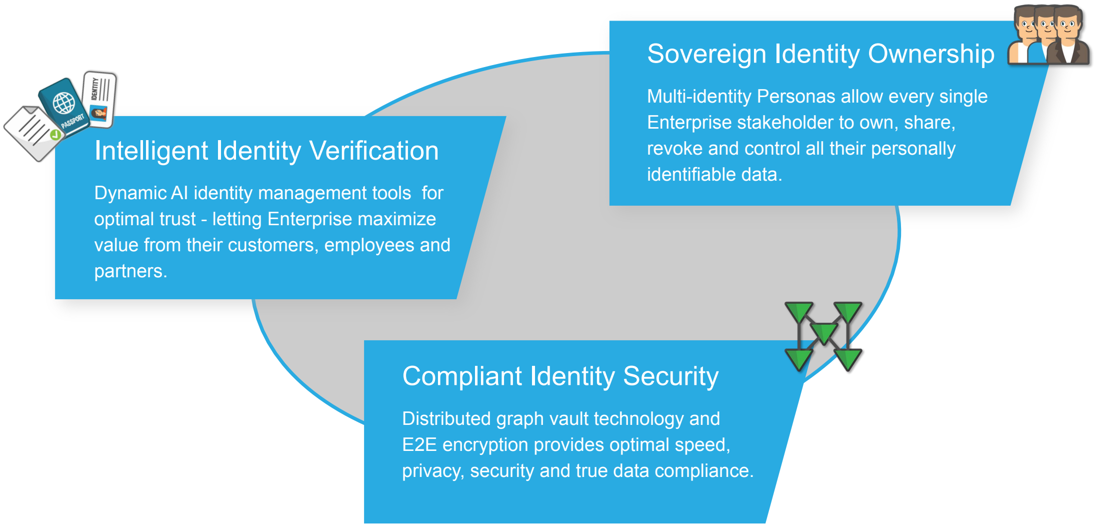
Truly Self-Sovereign Identity

SSI gives citizens complete control and ownership of all their personally identifiable information. It allows them to share only the necessary data for interactions, transactions and communication with other entities. Enterprises returning PPI to rightful-owning stakeholders are sending a strong, positive message about trust to everyone associated with the organisation.

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 keen to avoid unnecessary management storage costs and reduce regulatory risk common in centralised, federated and distributed ledger identity management systems.

Meanwhile, SSI allows each user securely create, store, manage, share, track, revoke and own all their PII. They can easily reuse verified identity and attestations - opening 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.

Leading end-to-end SSI solutions offer identity ownership, verification and secure compliance:



Sovereign Identity Ownership

Multi-identity Personas allow every single Enterprise stakeholder to own, share, revoke and control all their personally identifiable data.

Intelligent Identity Verification

Dynamic AI identity management tools for optimal trust - letting Enterprise maximize value from their customers, employees and partners.

Compliant Identity Security

Distributed graph vault technology and E2E encryption provides optimal speed, privacy, security and true data compliance.

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 apps (e.g. native digital identity wallets) leading SSI solutions provide users with robust, feature-rich encrypted functionality and services.

All identity, qualifications, references, certifications, memberships, entitlements, attestations and other personally identifiable data 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 should be created and shared on a field level. This includes government-issued identity cards, certification documents or an entirely new artefact. These artefacts can all be grouped into a single artefact for PII-intensive sharing activities, such as a mortgage application or a new patient sign-up. And self-provisioning is completely anonymous with users never needing to share any PII with other middlemen - or even 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 help prove who each individual is throughout the lifetime of the relationship.

SSI solutions allow organisations to securely authorise, authenticate and verify all types of users for all types of data transactions. It allows them to 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, 3rd party credit header verification or digitally-signed certifications from a lawyer.

Enterprise can also leverage out-of-bound biometrics for continuous authentication - whilst using conferred trust scoring that evaluates a user's credibility based on historical private and public network activity and behaviour. And 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 the core privacy by design principles. They provide adaptive, secure and controlled access to stakeholder identity and PII. They are compliant to global privacy regulation (e.g. GDPR, CCPA) offering true user data ownership - including real-time data consent, subject access request, revoking, the right to be forgotten. They should also offer real-time view of data transaction history & audit on a field level.

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

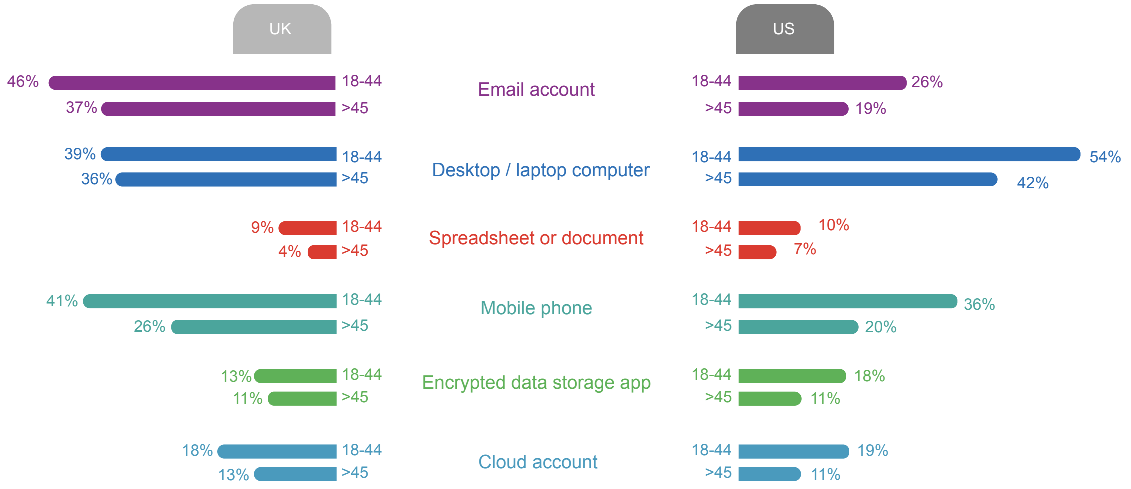
PII Ownership Perspectives in the UK and US

This research report offers a view of 1000 American and British citizens' digital identity activity, preferences and receptivity to SSI features. Key areas examined include:

- 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

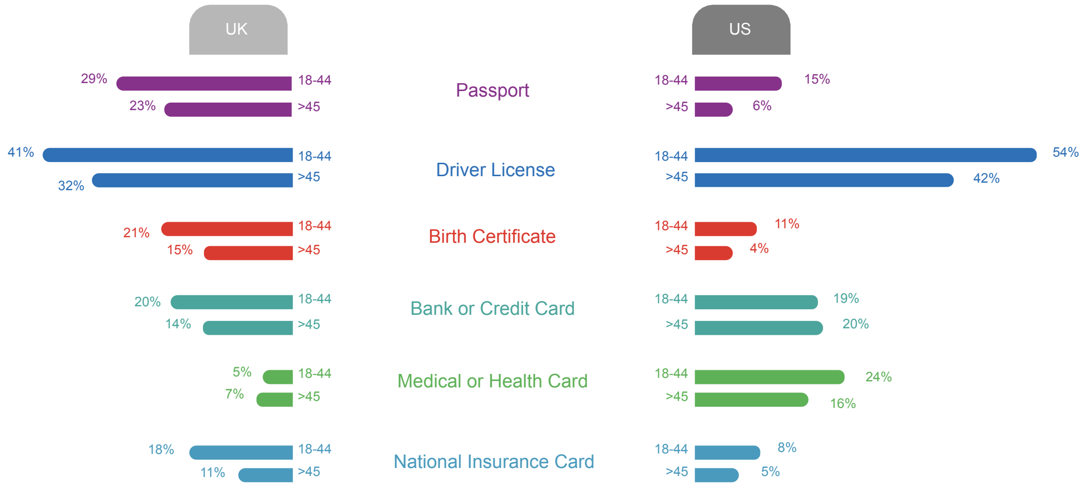
Current Digital Identity Management

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



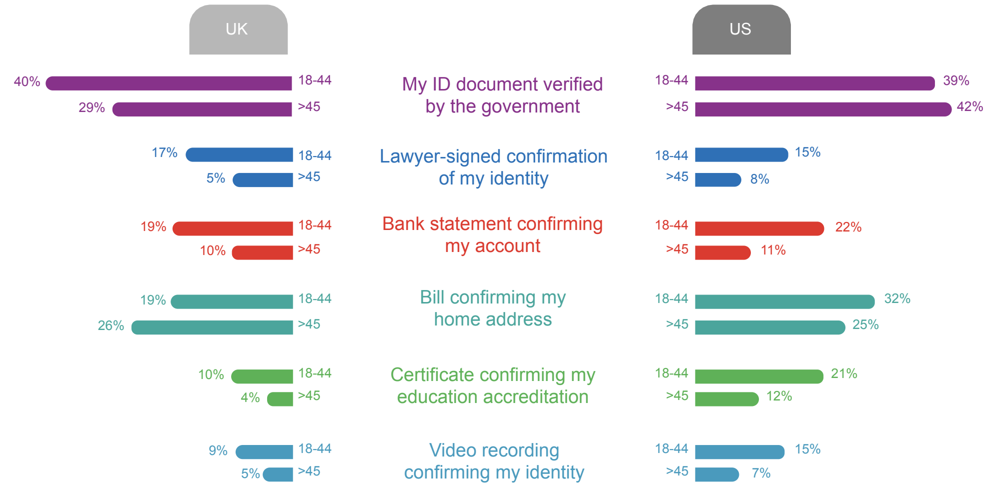
Digital Identity Document Sharing

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



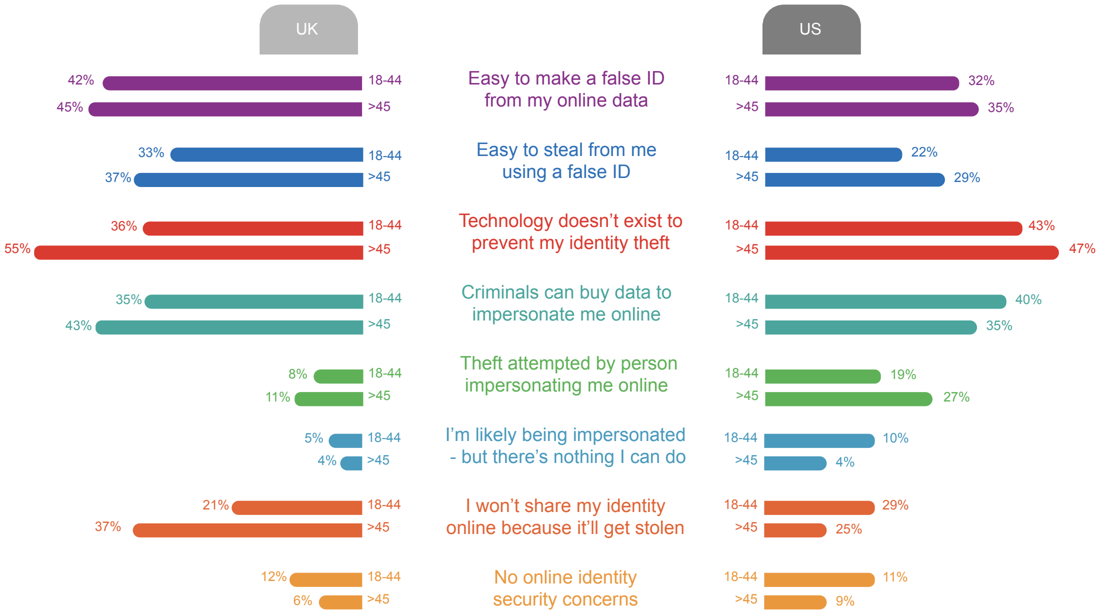
Stored Verified Identity Types

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.



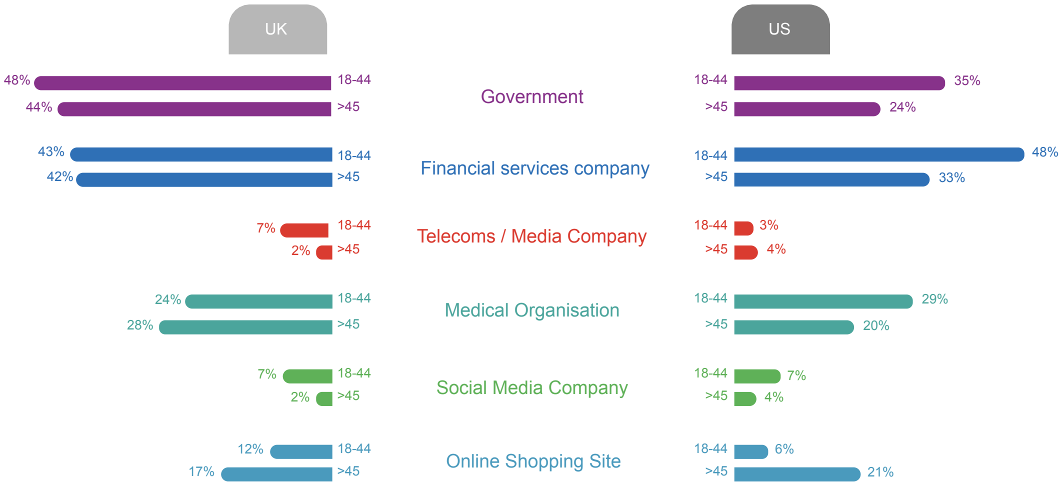
Digital Identity Security Concerns

Both US and UK citizens are concerned about their identity being hacked and used online. Over 41% say 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.



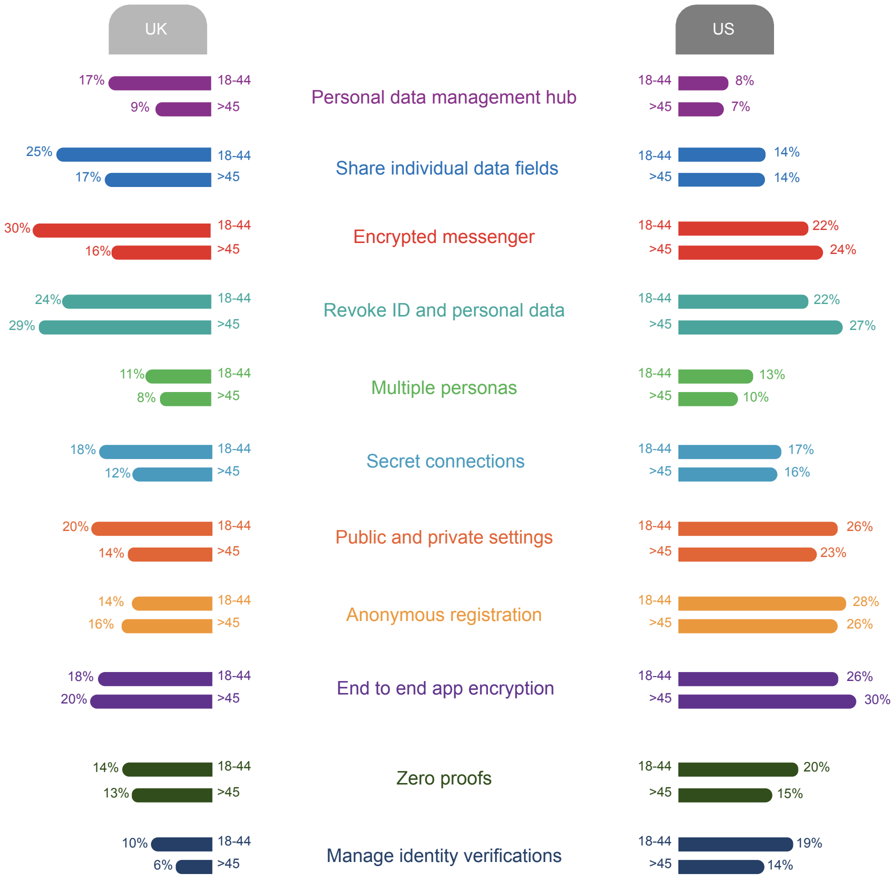
Trust in 3rd Parties for Digital Identity Management

The government is trusted more than financial institutions to manage users identity on their behalf in the UK, less so 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. Americans are particularly interested in end-to-end solution encryption and an anonymous registration that ensures no personal information is revealed during the onboarding process. And there is already some interest in both countries for having both public and private settings for sharing PII. British 18-44 year olds show a higher interest in encrypted messaging tools for sharing identity artefacts and other personal data.



Covid-19 and Medical Health Data Ownership in USA

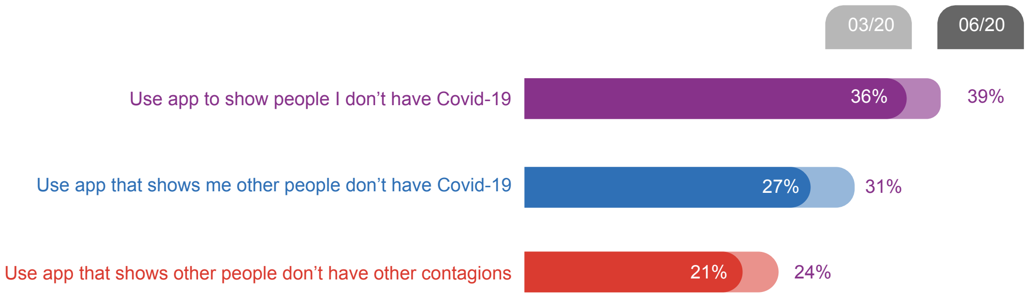
Global governments, companies and other organisations exercise emergency powers to access, analyse and make use of citizens' private information. In Taiwan, phone GPS triangulation is used by the police to ensure self-isolating people stay in their homes. In China, an Alipay app green QR code confirms people have tested negative for the virus during random street checks. In the UK, the National Health Service (NHS) is developing a heat-mapping surveillance app that traces people’s location to help them identify virus hotspots.

The security, privacy and user data monetization by rapidly growing video apps like Zoom and Houseparty are increasingly coming into question. And in the US, the Centre for Disease Control and Prevention (CDC) (always had) the power to not only detain citizens, force them into quarantine, but also access their identity and other private information on phones, email - even in their homes. Encouragingly new European Commission guidance outlines member nations building contact-tracing smartphone apps using notifications and bluetooth — and no personally identifiable data — to help fight the spread of COVID-19.

Research examining over 500 Americans views 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.

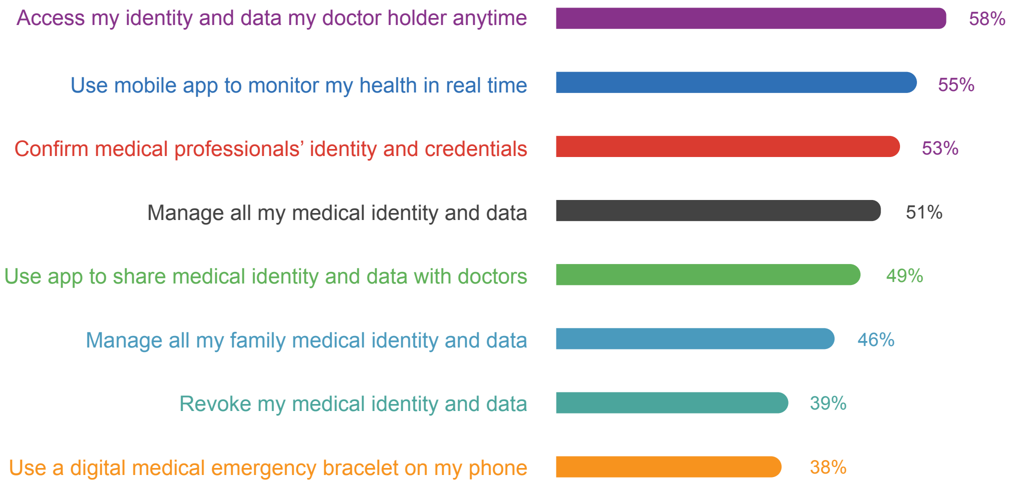
Covid-19 Test Result Sharing

Some Americans already want coronavirus test-result sharing. Interestingly, more want to prove to others that they’re negative (37%) versus demanding others prove to them they don’t carry Covid-19 (27%), In the upcoming year society will discover if this trend continues - and if it’s related to moral care for human life, job protection, online social reputation preservation or other factors.



Digital Health Identity Data Management

The survey reveals the demand for owning and sharing personally identifiable medical and health data is significant. Results show more Americans want self sovereign control to manage it themselves. They most want real-time access to shared medical information (59%), private health data tracking (55%) and management of all identity, prescriptions and other medical data on mobile devices (51%). Online identity and credentials checks to ensure medical professionals are who they say they are (53%) is also wanted. Only 11% of those surveyed aren't interested in any digital medical health data activities.



Digital Employment Data Ownership

The Covid-19 crisis is expected to have both a lasting medical and economic impact. It has led to excessive global unemployment. With more people trying to re-enter the labour market, there is a greater importance on having compliant personal data management tools needed for role applications.

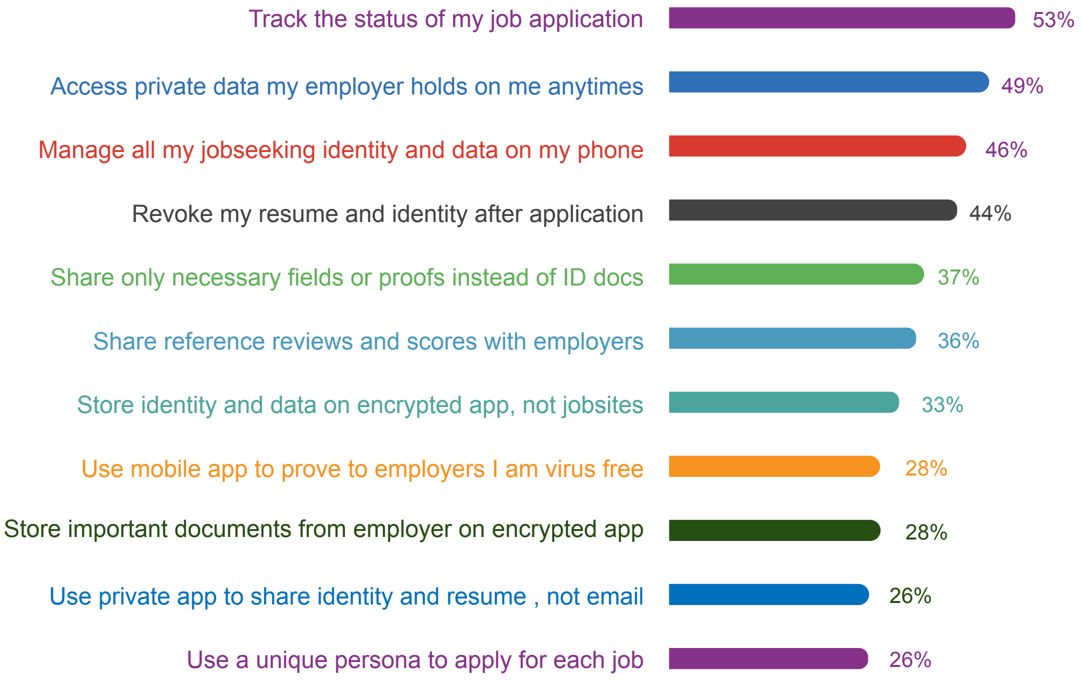
Market-leading solutions allow employers to shortlist candidates without ever touching any of their personal private data - offering real-time consent, revoking and right to be forgotten for every single application. They can request only necessary individual fields of personal data (zero-proofs) per role and application and let them share and revoke important employee artefacts, such as contracts, work ID and passwords. Proper compliance roles let employers allocate rights to HR professionals compliantly managing projects, roles and relevant applications. Employers can instantly access proper jobseeker artefacts for each application - securing every candidates' consented-for digitally-signed identity, resumes, qualifications, references, certifications, entitlements, claims, and other sensitive documents.

Proper solution features including candidate and identity management, attestation and referencing, project roles and rights, compliance management, analysis, templates, audit and history can increase the volume and quality of candidates which will reduce attrition rates. Each candidate has every single appropriate artefact to share each time, eliminating time wasted sharing artefacts back and forth. And built-in data protection roles let employers instantly return private data to jobseekers at each point of the application process, including submission, shortlisting, interview, hiring and role termination.

These solutions also offer identity personas letting jobseekers personalise every single application enabling them to be who you want to be and share what they want to share. They can privately share references, trust scoring, skills and experience reviews and medical test results. They can secure important employment artefacts, such as contracts, work identity and passwords after being employed. Revoking their identity and data upon application completion - reducing the risk they've unknowingly (and non-compliantly) shared data that can be harvested, analysed and sold on. Letting jobseekers centrally control and manage dozens of artefacts can improve application process and speed whilst gradually increasing the number of roles secured legally. Over time the government can see increased employment, more taxable contributions and improved employee protection as more jobs are secured legitimately.

Digital Employment PII and Identity Management in the US

Our research suggests Americans are interested in self sovereign employment identity and data sharing. Over 45% want to manage their own jobseeker artefacts and over a half want 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 a significant number (41%) want to revoke their private data - despite most never using this capability - given this feature isn't commonly available on mainstream social, commerce or other online sites. Interestingly some also want secure, private and sovereign alternatives to the current technology for managing and sharing personally identifiable information. One quarter would prefer to use their own private secure apps to share employment identity and data instead of email - whilst one half want self sovereign tools to manage such artefacts versus mainstream employment-related social media and job sites. And when they are in a job, nearly half want access to their private artefacts employers hold on them.



About Octopus.sh

Octopus.sh allows Enterprise to 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