Panelists

◊ Shannon Wu, *Identity Review*
◊ Jesse Leimgruber, *Bloom*
◊ Solomon Wong, *InterVISTAS Consulting*
◊ Tom Plofchan, *Pangiam*

Moderated by Erich Dylus, *Vedder Price*
Privacy: Some Context

- Expectation of privacy defines the scope of the applicability of the privacy protections of the Fourth Amendment (Subjective v. Objective)

- A right to privacy is a much broader concept, found in many legal systems

- Varying jurisdictions and customs, unique safety considerations, and other characteristics give airports very unique considerations as to privacy

- Public blockchain != private information exposure
  - Zero-knowledge proofs, attestations, self-sovereign identity, TEEs
Airport Blockchain Use Cases

- Digital identity solutions
- COVID-19 status attestation/contact tracing (verifiable immunity credentials)
- Service automation / airport vendor baselining
- Data Security

Data Storage v. Access: privacy **benefits** in decentralized data storage (mitigating honeypots) and/or queries (mitigating intercepts)
Digital Identity

- Blockchain enables truly self-sovereign identity
- Increasing scrutiny on how organizations are storing information
- Blockchain's public and private key pairing, digital proofs, etc. provides secure enterprise-level solutions in preventing tampering
# Digital Identity Landscape

An ecosystem of governments, organizations, data vendors and technology providers

## Digital Identity Ecosystem Body

Unifying important stakeholders for the future of digital identity.

## Governments and Organizations

- Health
- Transportation
- Finance
- National Identification Systems

## Data Attestors

<table>
<thead>
<tr>
<th>Raw Data Sources:</th>
<th>Identity Verification:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government Databases, Biometrics</td>
<td>Linking an individual to their information</td>
</tr>
</tbody>
</table>

## Identity Infrastructure Providers

<table>
<thead>
<tr>
<th>Customer Identity Service:</th>
<th>Authentication:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third party, identity-as-a-service</td>
<td>Proving the identity of a user</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Self-Sovereign Identity:</th>
<th>Login Providers:</th>
</tr>
</thead>
<tbody>
<tr>
<td>User controlled data and blockchain</td>
<td>Interface for account login/Single-Sign On</td>
</tr>
</tbody>
</table>

## Technology Standards

- NIST
- sovrin
- OpenID
- TRUST

---

## Aggregators:

- LexisNexis
- Experian
- TransUnion

## KYC Providers:

- Trulioo
- SOCIURE

## Authentication:

- Ipsidy
- RSA
- WIS@key

## Login Providers:

- Google
- Facebook
Digital Immunity Credentials

**Authenticity:** Unlike paper docs or certificates, Verifiable Credentials cannot be forged, transferred.

**Electronically Verifiable:** Being able to digitally verify immunity would reduce costs and workload, making it cheap and easy to issue and verify proof of immunity.

**Privacy:** Workers maintain full control and ownership of their test result and immunity credential, preserving privacy while providing cryptographic proof of authenticity.
Digital Immunity Credentials

**Share Remotely:** Verifiable Credentials can be easily shared remotely without the need for in-person verification or physically transferring documents, which poses an infection risk. Workers can share their immunity credentials online directly with employers or through job marketplaces.

**Portability:** An open-source Verifiable Credential standard would be interoperable between decentralized identity wallets. A number of members of the Decentralized Identity Foundation (DIF), including Bloom, are currently working on a standard and framework.
About Bloom

Founded in 2017, 1 Million+ people have created self sovereign identities with Bloom.

With 15+ data partnerships and IDs in almost every country, Bloom is the only live deployed end-to-end infrastructure covering DID creation, VC issuance, scaling, selective sharing, data partnerships, decentralized design, and real-world integrations critical to success in a live environment.

Background

- Founded out of Stanford University
- Previously founded successful identity verification company currently powering BBVA, Coinbase, and more
- Fmr. Chief Scientist of Experian Consumer & Advisors include Victor Nichols, former CEO of Experian North America
Privacy & Data Sharing Standards

**United States Government:** In 2020, the US Government's National Institute of Standards (NIST) published *A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems.*

Bloom's cryptographic solution for selectively and securely sharing elements was cited as the standard forward-looking solution for identity verification and credential management.

**Foundation & Consortia:** Bloom also sets the interoperable standards and leads core working groups for the Ethereum Foundation, Decentralized Identity Foundation, among others.

Clickwrap Privacy Statements
We Want Passengers to Remember the Fine Print

Exit / Boarding

The traveller is ready to take a journey outside the country. With previously collected identity attestations accessible from the mobile wallet on their smartphone, the traveller can share their information with the Border Management Agency for Exit Controls and with their airline for boarding.

The attestations contain the traveller’s information attributes, such as name and passport number, as well as the signature of the trusted issuing authority. This confirms the traveler’s information has been verified.

The traveler can share this information in advance, such as at the time of booking a journey. This allows advanced identification and verification of passengers, so processing is more efficient.

Key Steps:

• The traveller shares required identity attributes from their previously collected attestations with the Border Management Agency and their airline.

• The border/airline representative has the ability to review the identity attributes that were issued by the attestation authority.

• The traveler’s fingerprint is placed on the Exit Control/Boarding Gate.

• Upon reaching the gate, the traveler’s fingerprint is compared against the biometric placed on the gate.

• The traveler proceeds through the gate and boards without needing to present their physical passport.
Health measures/contact tracing creates new complexity

Local Health Authorities

National Health Authorities

Foreign Health Authorities

Submit Health

Airport Security

Airlines

Other Parties

InterVISTAS

Blockchain in Airports: Privacy Considerations
Three Key Directions on Privacy

Privacy by Design

Digital Transparency

Products to Limit Attacks

Blockchain in Airports: Privacy Considerations
A User-centric Approach to Privacy

Blockchain in Airports: Privacy Considerations
Privacy and Security, through Technology

- The Future of Travel as seamless and secure
- The Rights of Travelers to control their own data
- The Role of Government to validate, test, and protect
- An Industry-Specific Note on Privacy: Security v. Surveillance
The Future of Travel as Seamless and Secure

• **Seamlessness as a Vision**
  - Reduced Contact
  - Data Integration Enhances Both Security and Facilitation

• **Biometrics as a Backbone**

• **Advancing the Three Goals of Aviation**
  - Safety and Security
  - Efficiency
  - Passenger Experience
The Rights of Travelers to control their own data

- The Future of Data
  - Self-Sovereign
  - Protected
  - Zero-Knowledge Proof

The Role of Government

- Central Authority is Requisite in Aviation
- Governments Do Not Have Rights to Pattern-of-Life Data, but...
- They Do Have a Responsibility to Protect, and...
- Verifying Identity, Particularly When Crossing Borders, is Requisite to Protection
An Industry-Specific Note

Security v. Surveillance

- **Biometrics**: Verifying Identity vs. Locating, Tracking, or Surveilling
Q&A

- Shannon Wu, *Identity Review*
- Jesse Leimgruber, *Bloom*
- Solomon Wong, *InterVISTAS Consulting*
- Tom Plofchan, *Pangiam*

Moderated by Erich Dylus, *Vedder Price*