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 enterpriselevel solutions in preventing tampering

Digital Identity Landscape

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





Verifiable Immunity Credentials

to Help Fight COVID-19

Digital Immunity Credentials

Authenticity: Unlike paper docs or certificates, Verifiable Credentials can not 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

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

A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems

Leit Lesavar Priam Varin Press Mill Michael Davidson James Mook Computer Society Division Information Technology Laboratory

January 14, 2020

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.01142020



Source: United States Government (NIST): <u>A Taxonomic Approach to Understanding Emerging Blockchain</u> <u>Identity Management Systems.</u>

Clickwrap Privacy Statements

The second of the late of the second second

 Present a control to de control de vers for the same forget and control desce data to the descent descent and on accounting to the the same is compared and and additional and additional and accounting the same is also a same and and additional and additional and and additional and performance and performance and a same and additional and additional and additional and performance and performance and additional and additional and additional additional additional additional additional before to truth them performs and additional additional additional additional and additional additeditional additional additionad additionad additional addition

The second for the second second is a first of the second se

New York, Different Scherberg, Children and Scherberg, Scherberg,

in court adore, "the latter has see whency or an an or of the exercise and desceptions are in that contribute although them is served, actual and action and we country that is any overall an aptive best receil as and water

We have developed with a solution process of inclusions and an installa due of the biologic default to ensure large an expert of the time data has been used. Also, by of biologic data for some time TCOD and an antimativa has been used to that the data of the former some and the time time of the solution of the solution of the time and the time of the solution of the solution of the solution of the solution of the former solution and the solution of the solution of the solution of the time of the solution of the solution of the solution of the solution of the time of the solution of the sol

Densit invaries a true range and which true or their partners is the course of their relation server true or an anise two stands well-the location or data? Along a data

AWS Customer Agreement

Check here to indicate that you have read and agree to the terms of the AWS Customer Agreement

Create Account and Continue

Check 📃 to state you have read and agree to our Terms and Conditions









To continue playing, you need to confirm that you agree to our Terms of Service and have read our Privacy Policy

Terms of Service

Privacy Policy



We Want Passengers to Remember the Fine Print



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

КTD

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 traveller's information has been verified.

The traveller 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 enrolment authority

•The travellers biometric is placed on the Exit Control / Boarding Gate

 Upon reaching the gate, the travellers face is compared against the biometric placed on the gate

 The traveller proceeds through the gate and boards without needing to present their physical passport





Privacy Impact Assessment for the

Traveler Verification Service

DHS/CBP/PIA-056

November 14, 2018

Contact Point Colleen Manaher Planning, Program Analysis and Evaluation (PPAE) Office of Field Operations U.S. Customs and Border Protection (202) 344-3003

> <u>Reviewing Official</u> Philip S. Kaplan Chief Privacy Officer Department of Homeland Security (202) 343-1717

Health measures/contact tracing creates new complexity

Local Health Authorities

National Health Authorities

Foreign Health Authorities



Airport Security

Airlines

Other Parties

Three Key Directions on Privacy

Privacy by Design

Digital Transparency

Products to Limit Attacks







A User-centric Approach to Privacy







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 **The Role of Government** control their own data

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

- **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







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

Moderated by Erich Dylus, Vedder Price