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 ecosytem of governments, organizations, data vendors and technology providers

Digital Identity Ecosystem Body

Unifying important stakeholders for the future of digital identity.

Identity Review

Governments and Organizations

- Health
- Transportation
- Finance
- National Identification Systems

Data Attestors

Raw Data Sources:

Government Databases, Biometrics

Identity Verification:

Linking an individual to their information

MiTek, onfido, JUMIO

Aggregators:

Provider of information sources

LexisNexis, experian, TransUnion

KYC Providers:

Identifying individuals for account opening

Trulioo, SOCURE

Identity Infrastructure Providers

Customer Identity Service:

Third party, identity-as-a-service

PING, onelogin, okta

Authentication:

Proving the identity of a user

Ipsidy, RSA, WISeKey

Self-Sovereign Identity:

User controlled data and blockchain

BLOCKSTACK, evernym, Bloom

Login Providers:

Interface for account login/Single-Sign On

Google, Facebook

Technology Standards

NIST, sovrin, OpenID, TRUST Over IP FOUNDATION

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

Cognito — Previously founded successful identity verification company currently powering BBVA, Coinbase, and more

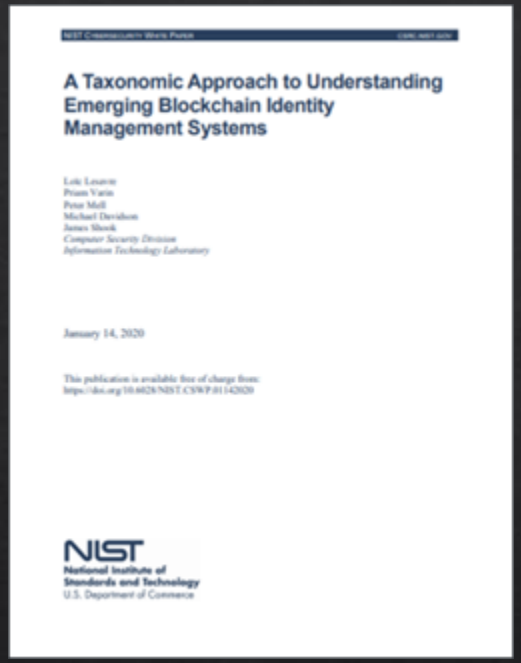
experian — Fmr. Chief Scientist of Experian Consumer & Advisors include Victor Nichols, former CEO of Experian North America

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

Lois Lesavre
Priam Varin
Peter Mell
Michael Davidson
James Shook
Computer Security Division
Information Technology Laboratory

January 14, 2020

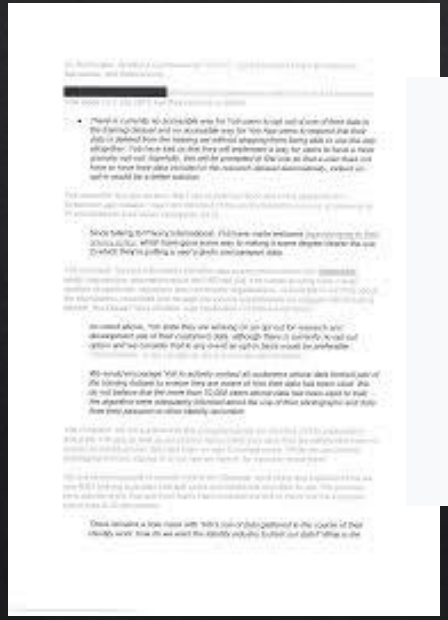
This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.01142020

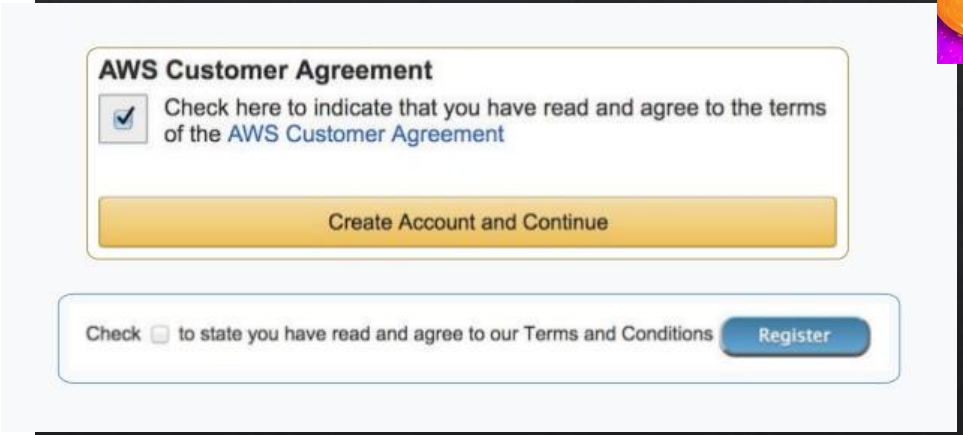
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

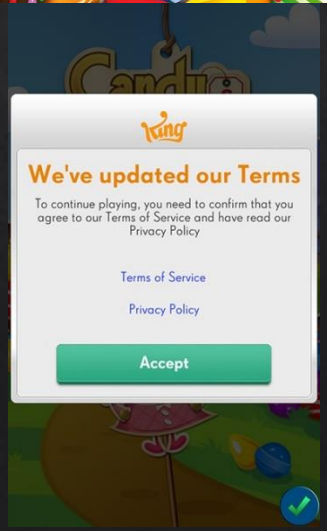
DIF

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

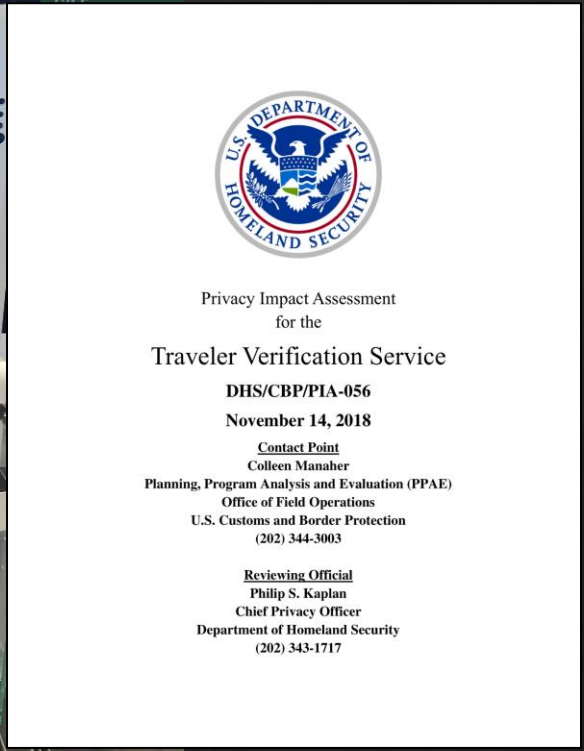
Clickwrap Privacy Statements







We Want Passengers to Remember the Fine Print



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

Reviewing Official
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

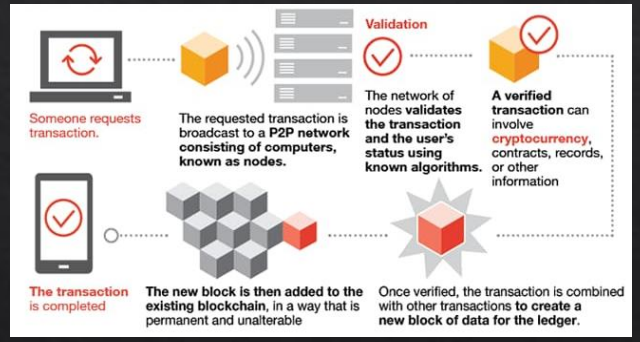
Blockchain in Airports: Privacy Considerations

Three Key Directions on Privacy

Privacy by Design

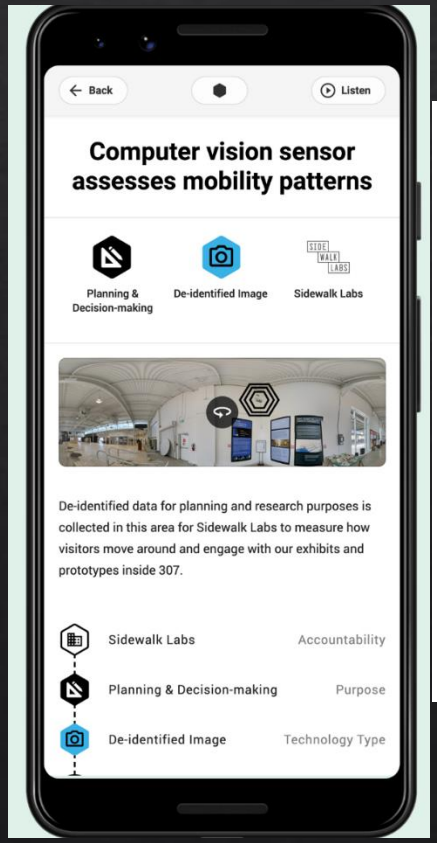
Digital Transparency

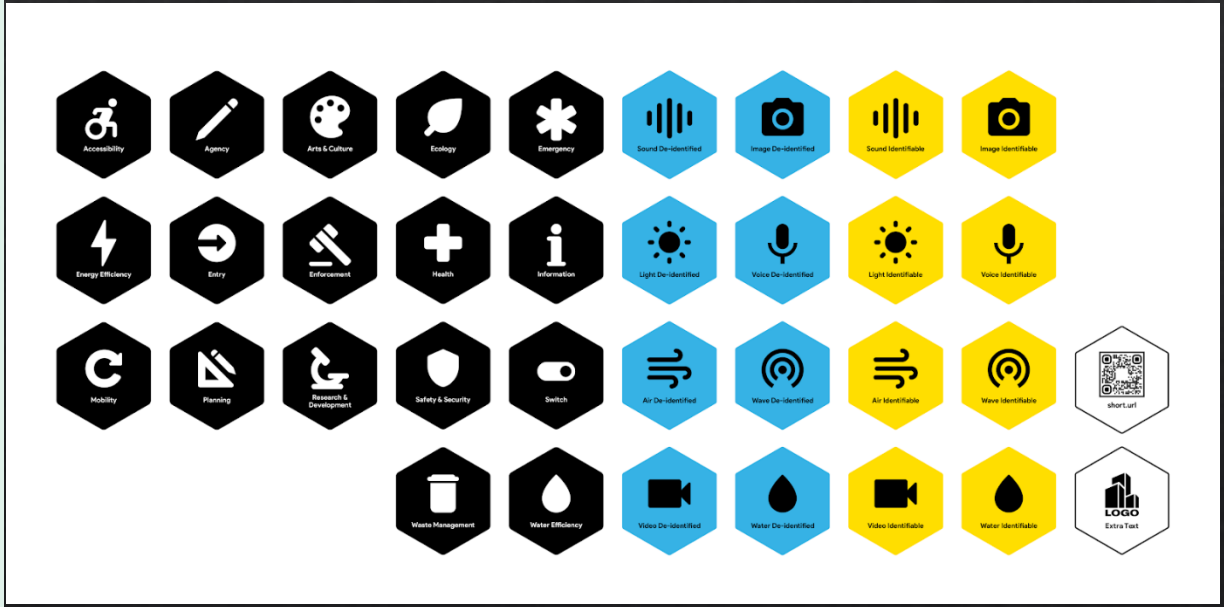
Products to Limit Attacks



Blockchain in Airports: Privacy Considerations

A User-centric Approach to Privacy





Blockchain in Airports: Privacy Considerations

PANGIAM

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*