



MEET THE METAVERSE!

A Reality Check for Insights.

Thank you to our Sponsors!



MEET THE
METaverse!
A Reality Check for Insights.

Session 3

13:30

Session 3: The Participant Focus



13:30

ESOMAR perspectives on privacy & profession.

By **Dr Parves Khan**, Director General & CEO, ESOMAR



14:00

Metaverse and identity.

By **Kerry Frank**, Head of Digital Identity, Snickerdoodle Labs | Oxford Pershing Square Scholar



14:30

Metaverse and the impact for participant engagement.

By **Betty Adamou**, Author, Games & Gamification in Market Research

15:00

Tea (Refreshments & Networking)



MEET THE
METaverse!
A Reality Check for Insights.

Digital Identity: Perspectives from Web2 and Web3

Kerry Frank

Head of Digital Identity @ Snickerdoodle Labs

Kerry@SnickerdoodleLabs.io



In Today's Presentation:

- 1 **Brief Overview of Digital Identity and Web2/Web3**
- 2 **Why Web2 Fails Digital Identity and is not Salvageable**
- 3 **Web3 and Digital Identity: Better Fit-for-Purpose**
- 4 **Industry Examples: Snickerdoodle, Compliance, and Market Research**
- 5 **Questions**

Introduction to Digital Identity

Digital identity is the aggregation of identity attributes when expressed digitally...

Of these attributes, some are more or less fundamental to establishing a differentiable identity that allows me to participate in wider society (thus requiring different levels of assurance to authenticate each data attribute).

INHERENT

Age

Fingerprints

Place of birth

Eye color



ACCUMULATED

Behaviors

Preferences

Online browsing data

Geolocation history data



ASSIGNED

Government or Tax ID

Student number

Phone number

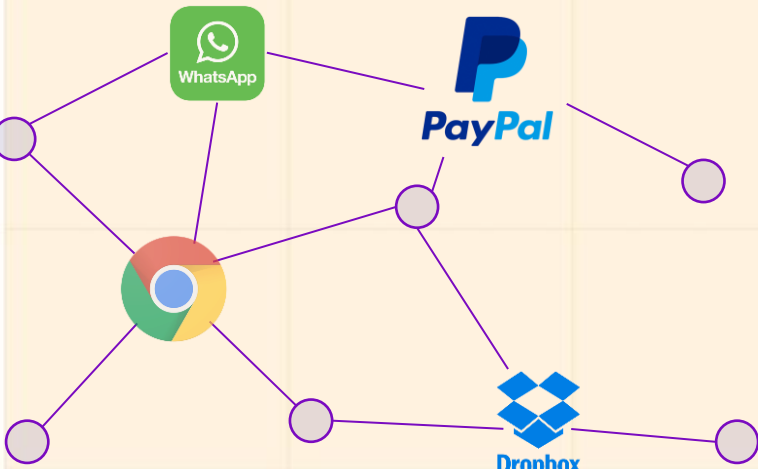
Email address



What's the Difference?

Web2

- **STREAMLINED:** Web2 introduced us to the internet and interactions we know today, bringing Web1 to the masses
- **USER PARTICIPATION AND INTERACTION:** 'Authoritarian' platforms control the user experience and the nature of their interactions
- **CENTRALIZED:** User data and effective ownership is stored centrally on the platform providers data, with limited efficiency for sharing outside of APIs



Web3

- **DECENTRALIZED:** Ownership is distributed among users – data is under the sole control of its owner, regardless of where its stored
- **PERMISSIONLESS:** Anyone can participate or access without having to seek permission from a government, service provider, or other gatekeeper
- **TRUSTLESS:** Users can interact directly – in public or in private – without the need to rely on a third party as an intermediary



Why **Web2** Fails Identity: 4 Ps Model



PRIVATE: Control over one's identity, data, and its permissioning

- Data ownership is relegated to corporations, governments, or organizations; there might be fees to export identity data (passports, transcripts)
- Many data monopolies build moats around their data arsenals
- Opting out of 3rd party sharing or selling of data is buried or exceptions are carved out through the T&Cs



PERSISTENT: Identity data exists indefinitely beyond confines of institution that originally captured it

- Data is only persistent so long as an institution is still solvent or functional:
 - If my credit card provider closes shop tomorrow, I lose my credit and account transaction history
 - If my country collapses or descends into civil war, I would need to register for a new sovereign identity with the UNHCR upon escape



PORTABLE: Underlying data is both accessible across several mediums and easily shared to relevant 3rd parties

- Data resides in centralized databases - users are at the mercy of each institution to facilitate data access and transfer
- Disclosure to 3rd parties of identity data can be a painful and tedious process (ex. medical data)
- Even though GDPR and CCPA specify exported data must be useable in a structured and machine readable format, this standard is rarely upheld



PERSONAL: Data is unique to identity holder

- Due to siloed nature of Web2 datasets, many identity profiles cannot claim to be unique (they will have a unique identifier like a number or email to facilitate authorization and access rights)
 - Social media profiles are easily replicated by copying pictures or posts for social phishing
 - Rampant financial identity fraud from Equifax leak

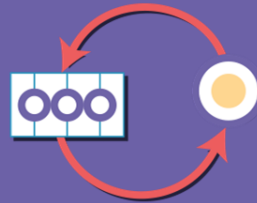
Innovation in **Web2** Identity Models Falls Short

Web 2 Identity Management



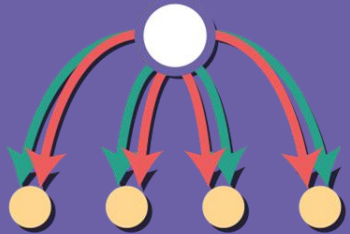
Internal Identity Management

A single entity acts as both IdP and RP



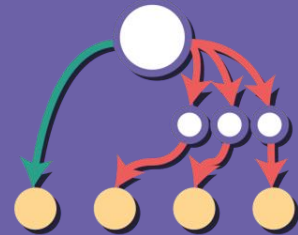
External Authentication

Multiple IdPs authenticate users to a single RP



Centralized Identity

A single IdP serves multiple RPs



Federated Authentication

A set number of IdPs authenticate users to multiple RPs



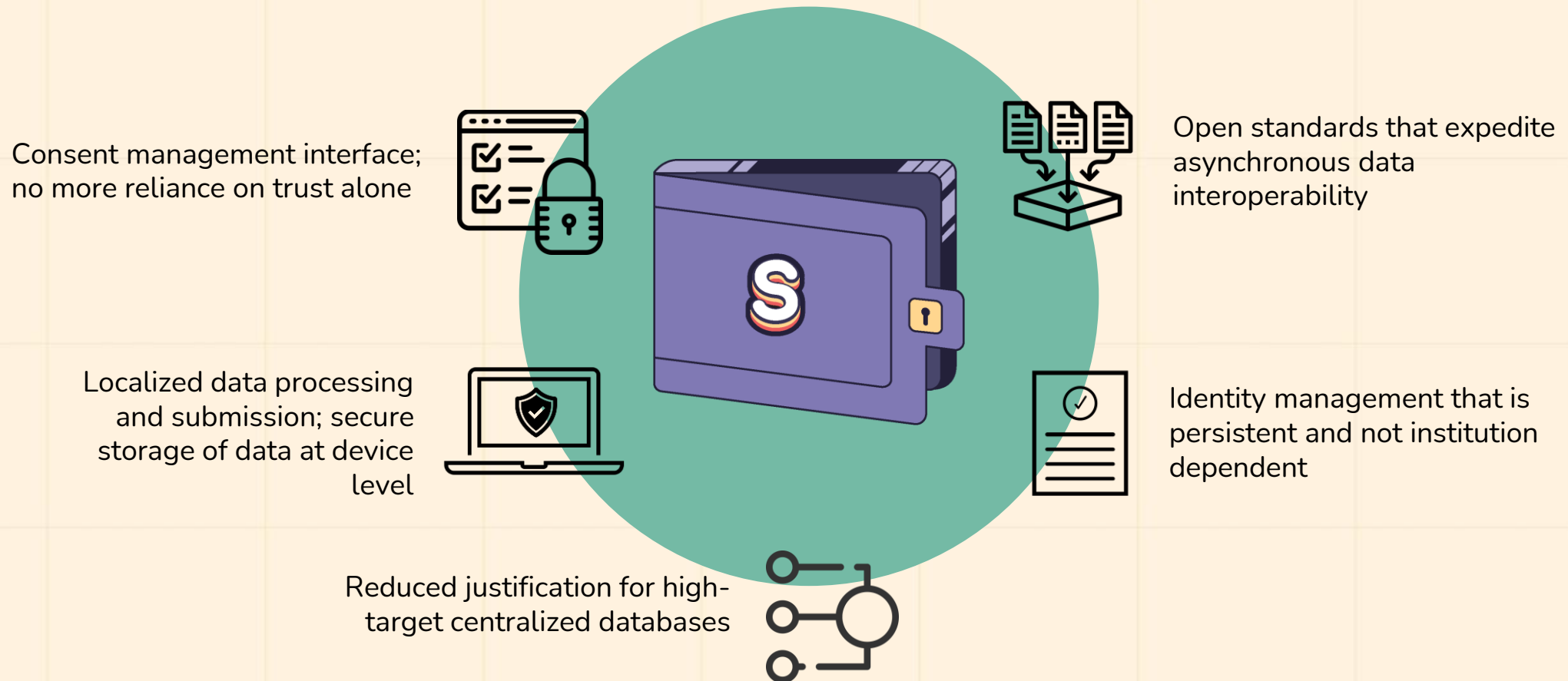
Food for Thought...

What is strange about these data attribute flows?



Digital Identity in **Web3**: A New Path

A **holistic, hybrid** approach to Digital Identity in Web 3 utilizes a **Data Wallet** as the primary end-user client interface, deputizes end users as the heart of the data sharing ecosystem, and shifts data ownership by enabling **users** to **control and consent to the collection, storage, and usage of their data**.



Web3: Principles of Identity Management

The 12 guiding principles of Self-Sovereign Identity Movement (SSI)...

SSI argues only web3 can truly capacitate multiple identity products

AGENCY



Representation



Delegation



Equity and inclusion



Usability, accessibility and consistency

AUTONOMY



Participation



Decentralization



Inoperability



Portability

INTEGRITY



Security



Verifiability and authenticity



Privacy and minimal disclosure



Transparency

Web3 Data Containers and Use Cases

Pre-Existing
Web2 & Web3 Data

Authenticated Self Imported Data

- Proven ownership of data via APIs e.g. Web3 activity via Metamask integration

Unauthenticated Self Imported Data

- No proven ownership of data via APIs e.g. Uploading data exported from Facebook

Digital Asset
Ownership

Non-Fungible Token (NFT)

- Unique tokenized digital assets with with specific smart contract address and token ID pair e.g. tickets, intermediary fee content (music)

Non-Sensitive
Social-Oriented
Interactions

Soul-Bound Token

- Non-transferrable NFT e.g. an attendance badge, charitable giving acknowledgement, symbolic credentials

All Sensitive Data
(not on ledger)

Verifiable Credentials

- Off-chain identity claims cryptographically signed by an issuer and stored in digital wallet on chain-verifiable data registry e.g. medical records

Web3: Industry Example... A Data Wallet



***Snickerdoodle
Data Wallet***

**Own & monetize
your data**

Data Insights... Visualized by Anonymized Dashboards

Snickerdoodle Insights Portal

Get usable
customer insights



Web3... an Enabler of Compliant Data Models

Web3 is strongly positioned to be the vehicle capacitating regulatory **compliance** embodied by **GDPR** and **CCPA** with great adaptability for continued progress and changes in **Digital Identity or data regulations globally**

Some rights GDPR/CCPA enshrine:

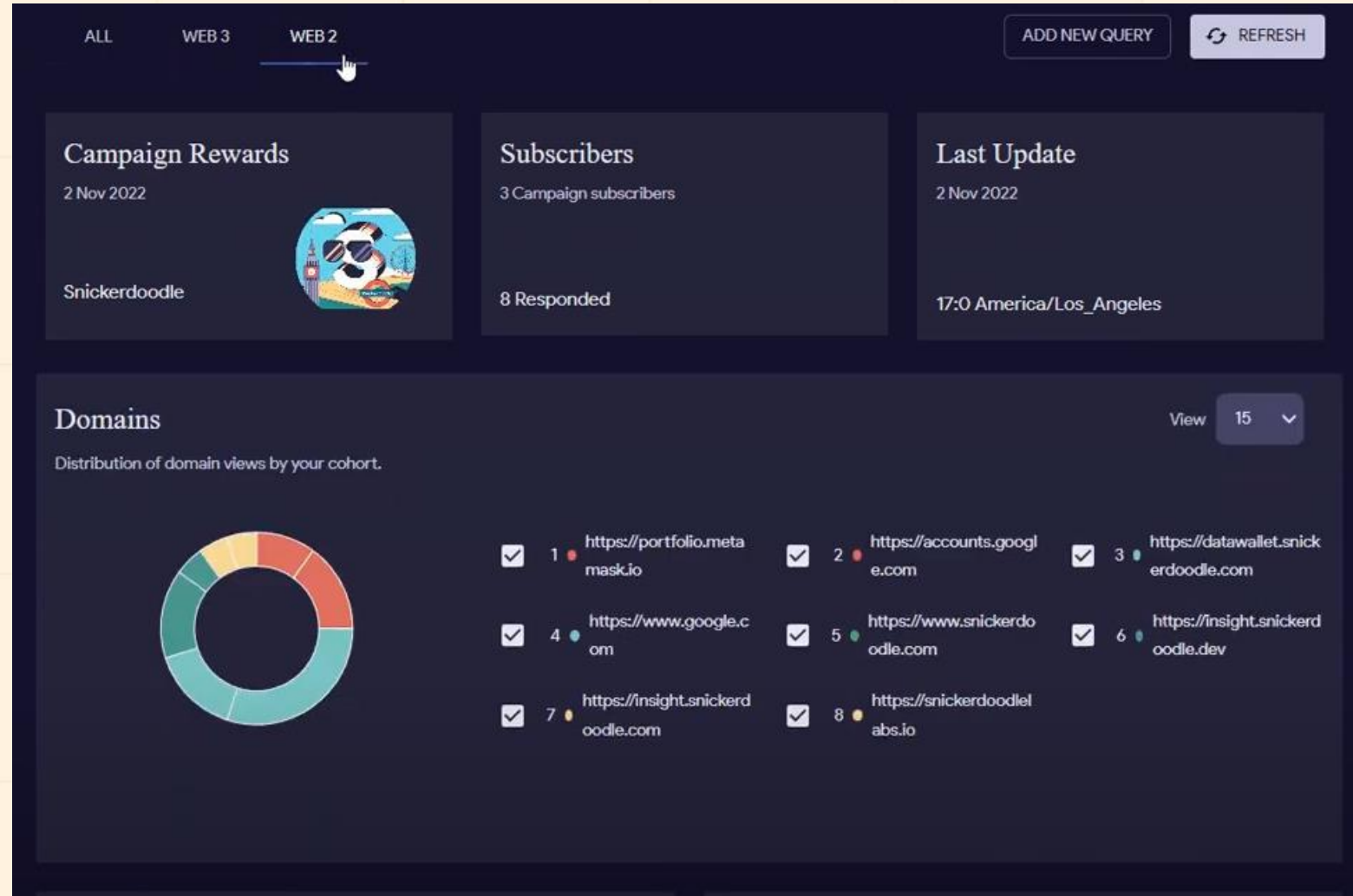
- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object

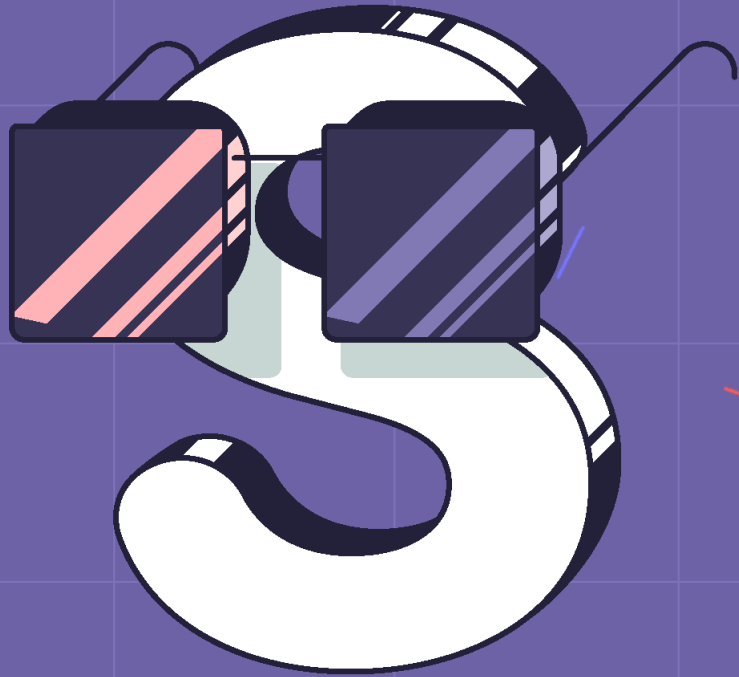
How Web3 encapsulates these rights and implications:

- Data is stored at the user level, which streamlines right of access, rectification, and data portability
- Any initiation of data transfer must be permissioned by the end user, fulfilling the right to restrict processing or the right to object
- Users can permission ongoing access to and queries of underlying data or take them away - either way the need for centralized databases is reduced
- Web3 architecture organically builds in data access authorization and distribution rights, so enterprises have less proof of burden that they acquired consent

Consumer Market Research in a **Web3** World

- **OPT-IN MODEL:** End-user market research will have to align with an opt-in model and ongoing access permissioning instead of an opt-out model (i.e. a consent based data sharing ecosystem)
- **DECENTRALIZED DATABASES:** Market research can no longer rely on large centralized repositories of information
- **PRIVACY OPTIMIZED DATASETS:** Data dashboards are anonymized and prevent individual triangulation but still allow for actionable insights
- **COMPENSATION FOR DATA:** End consumers are compensated and benefit from some of the value created in the data sharing economy





Thank You

Questions?



MEET THE METAVERSE!

A Reality Check for Insights.