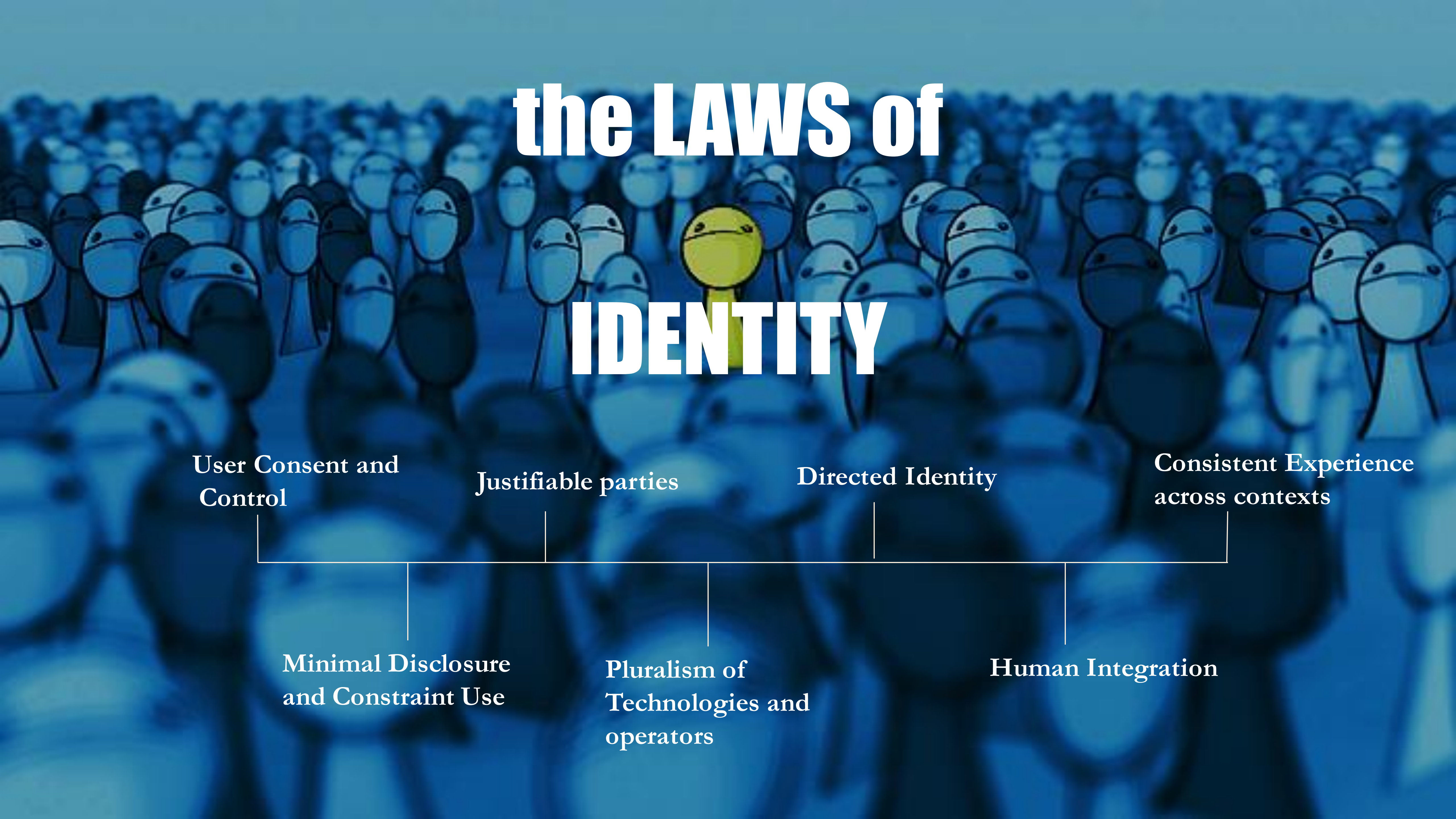


the LAWS of IDENTITY

- User Consent and Control
- Minimal Disclosure and Constraint Use
- Justifiable parties
- Pluralism of Technologies and operators
- Directed Identity
- Human Integration
- Consistent Experience across contexts

Introduction

- *"You want me to tell you about heaven before I died"*

  ~ Kim Cameron, when asked to describe the perfect Identity system.

- Was a Computer Scientist.
- Authored the 7 laws of identity.
- Worked at Microsoft as the Architect of Identity.
- Architect of Microsoft's Active Directory.

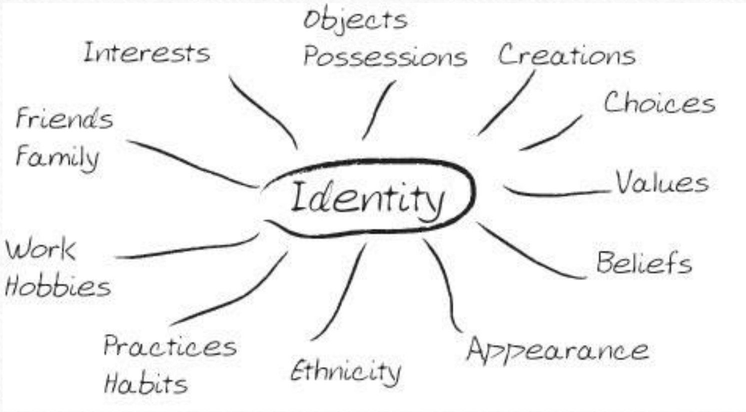
Digital Identity

- *Identity – The fact of being who or what a person or thing is.*

~ Oxford Dictionary

- **Digital Identity** – Set of **claims** made by one **digital subject** about itself or another digital subject.
- **Digital Subject** – Person or thing(computers, etc.) existing in the digital realm.
- **Claim** – An assertion of the truth of something

- Claims may convey personal identifying information (name, date of birth…etc.)



What makes up your identity?

Matt Murdock or Dare Devil or lawyer

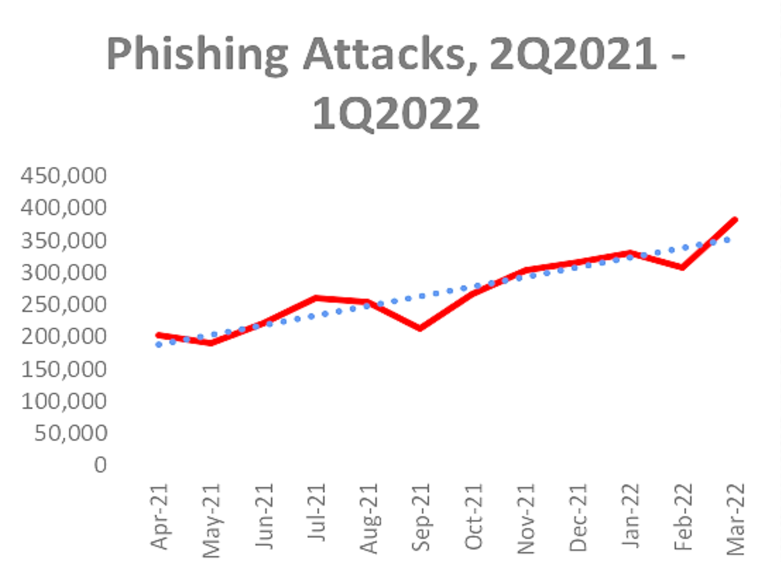
There Is No Identity Layer

- *The internet was built without a way to know who and what you are connecting to.*

- In most cases, you do not know the person or organization responsible for what you are connecting to.

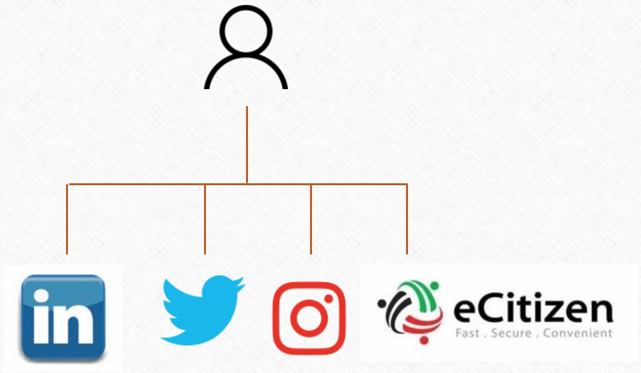
- [Free Identity Verification Service for Consumers | Medium]

- Every system has its own approach to identity. An average user has 100 passwords.(NordPass)

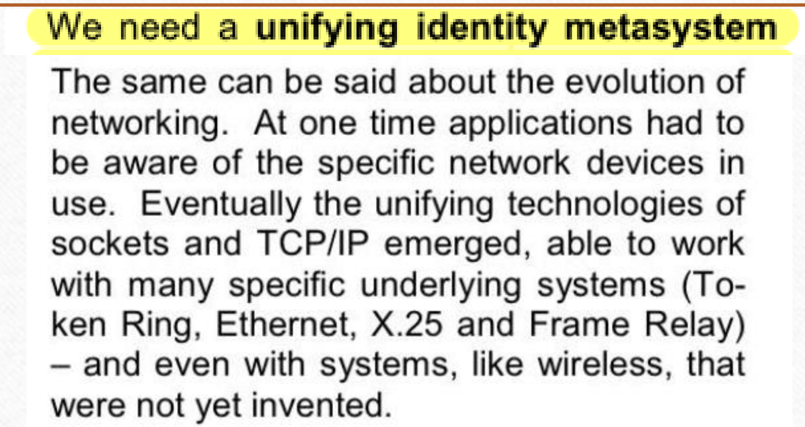


Creating An Identity Layer is Difficult

- Little agreement on what it should be and how it should run.
- Digital identity is related to context.

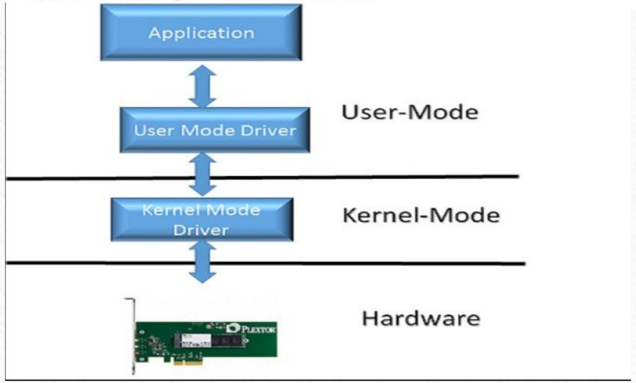


Digital identities to access different contexts.



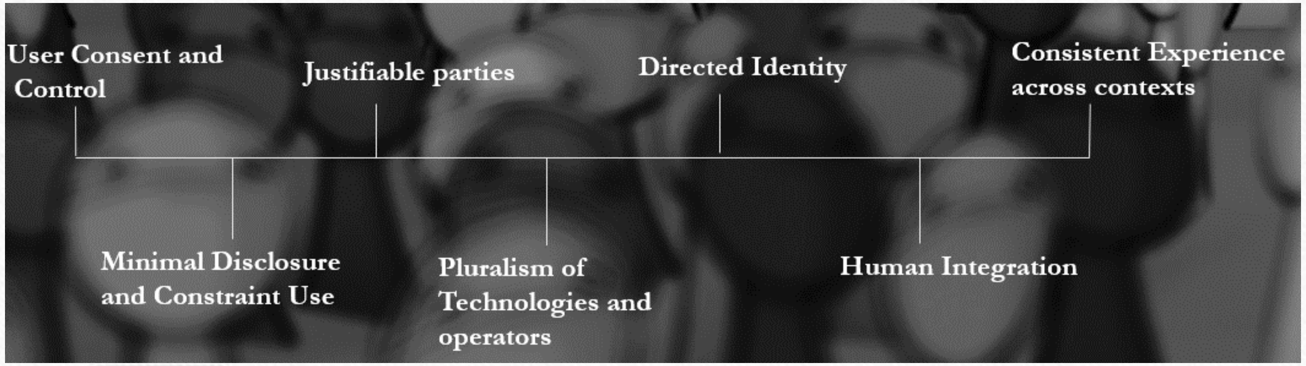
We need a unifying identity metasystem

The same can be said about the evolution of networking. At one time applications had to be aware of the specific network devices in use. Eventually the unifying technologies of sockets and TCP/IP emerged, able to work with many specific underlying systems (Token Ring, Ethernet, X.25 and Frame Relay) – and even with systems, like wireless, that were not yet invented.



The Laws of Identity

- The laws define the architecture of the internet's missing identity layer
- Each law is an architectural principle guiding the construction of such a system.
- Are testable – Allow prediction of outcomes. They have been tested consistently.
- Are objective – Existed and operated before they were formulated. (Microsoft Passport)



User Consent and Control

Minimal Disclosure and Constraint Use

Justifiable parties

Pluralism of Technologies and operators

Directed Identity

Human Integration

Consistent Experience across contexts

Law 1: User Control and Consent

- *Technical identity systems must only reveal information identifying a user with the user's consent.*
- User's control – Digital identity used, and information released.
- Protect the user against deception – verifying identity of systems who ask for information.
- Inform user when their internet behavior is being tracked.
- Allows the metasystem to remember the user's decision.

Law 2: Minimal Disclosure for a Constraint Use

- *The solution which discloses the least amount of identifying information and best limits its use is the most stable long-term solution.*
- Build systems that acknowledge that a **breach is always possible for identifying information.**
- The value of identifying information decreases as the amount decreases. (**Less attractive for identity theft**)

- Store information on a **need-to-know** basis and a **need to retain basis.**

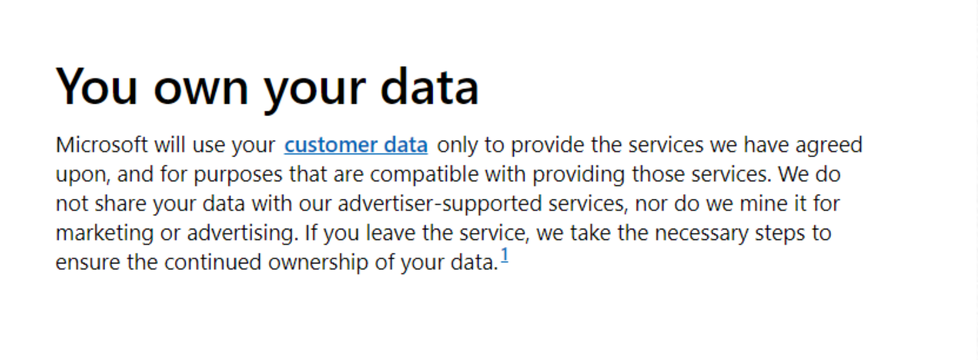
Example:

- If a system requires proof of age, acquire and store the age category rather than the birth date.

Law 3: Justifiable Parties

- *Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.*
- The user is aware of the parties or party with whom they are interacting while sharing information.

- A policy statement should be provided about information use.



You own your data

Microsoft will use your customer data only to provide the services we have agreed upon, and for purposes that are compatible with providing those services. We do not share your data with our advertiser-supported services, nor do we mine it for marketing or advertising. If you leave the service, we take the necessary steps to ensure the continued ownership of your data.[1]

Derived from Data management at Microsoft – Microsoft Security

Law 4: Directed Identity

- *A universal identity system must support both omni-directional identifiers for use by public entities and unidirectional identifiers for use by private entities thus facilitating discovery while preventing unnecessary release of correlation handles.*
- Identity has direction. Public identifiers can be thought of as a beacon.
- Bluetooth and other technologies have so far not conformed to this law. They use public beacons for private entities.

Example:

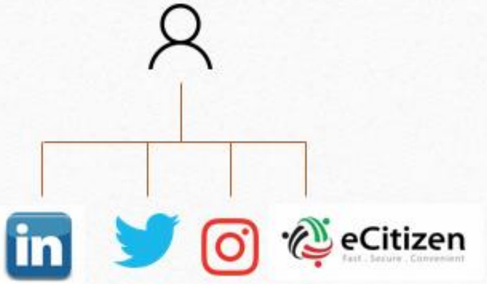
- If you visit a corporate website, you can use the identity beacon of the site (public URL) to decide whether you will connect to it.
- Your system then creates a unidirectional identity to connect with that site and no other.

Law 5: Pluralism of Technologies and Operators

- *A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.*
- A universal system must embrace differentiation.
- A user is simultaneously in different contexts – a citizen – employee – customer – avatar
- Individuals and organizations should be able to select appropriate identity providers and features.

Example:

- Government digital identities work for government services. Employers and employees in most cases would not use the government identity for work.
- Identity systems should be created to offer different (and contradictory) features.



Law 6: Human Integration

- *The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.*
- Is the channel between the browser's display and the brain of the user adequately protected?
- It is under attack through phishing and pharming.

- What identities is the user dealing with as they navigate the web. Is the identity information conveyed in an understandable way?

Example:

- United Airlines channel 9. Allows conversations between the cockpit and air traffic control. Participants don't chat. The channel is important, technical, and highly focused. When things go wrong, the human can easily understand and respond.

Law 7: Consistency Across Contexts

- *The unifying identity metasystem must guarantee its users a simple consistent experience while enabling separation of contexts through multiple operators and technologies.*
- **Thingify** digital identities. Make them into things a user can see on the desktop, add, delete, select, share.
- Like icons and lists that represent folders and documents.

- The different digital identities then become part of an integrated world which respects the need for independent contexts.

1. Properties are specified by a webserver.
2. Matching thingified digital identities are displayed to the user. They select and use them to understand information being requested.
3. The user then has control of what is being released.

Conclusion

- Those who work with identity need to obey the laws of identity.
- Otherwise, side-effects are created that eventually undermine all resulting technology.
- It is akin to civil engineers not obeying the laws of gravity.

- By following the **laws of identity**, we can build a unifying identity metasystem that is universally accepted and enduring.

- *"You can never be too paranoid about identity"*

~ Kim Cameron

Questions/Comments/Discussion

Thank YOU!

Resources Used.

- The Laws of Identity
- Kim Cameron (Wikipedia)
- The Internet Was Built Without An Identity Layer
- Video Recording of the Discussion of the Laws With Kim Cameron
- Average user number of passwords
- Phishing Attacks Hit an All-Time High in Q1 2022 (phishingtackle.com)
- Images sourced from Bing image searches.