

Laws of Identity

Identity Management & Federation 2019

Laws of Identity

- In 2009, Kim Cameron wrote a paper entitled “The Laws of Identity” in which he introduced seven fundamental truisms that every successful identity system must honour.
- Kim Cameron was Microsoft’s Architect of Identity and his 7 laws were an introspective look at Microsoft’s failed Passport system.
- They still hold true ten years later...

<http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf>

1) User Control and Consent

- Technical identity systems must only reveal information identifying a user with the user's consent

Now required by law (POPI Act; GDPR)

2) Minimal Disclosure for a Constrained Use

- The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution.

Now required by law (POPI Act; GDPR)

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.

Now required by law (POPI Act; GDPR)

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.

5) Pluralism of Operators and Technologies

- A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.

6) Human Integration

- The universal identity metasytem 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.

7) Consistent Experience Across Contexts

- The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.
- RA21: Resource Access for the 21st Century