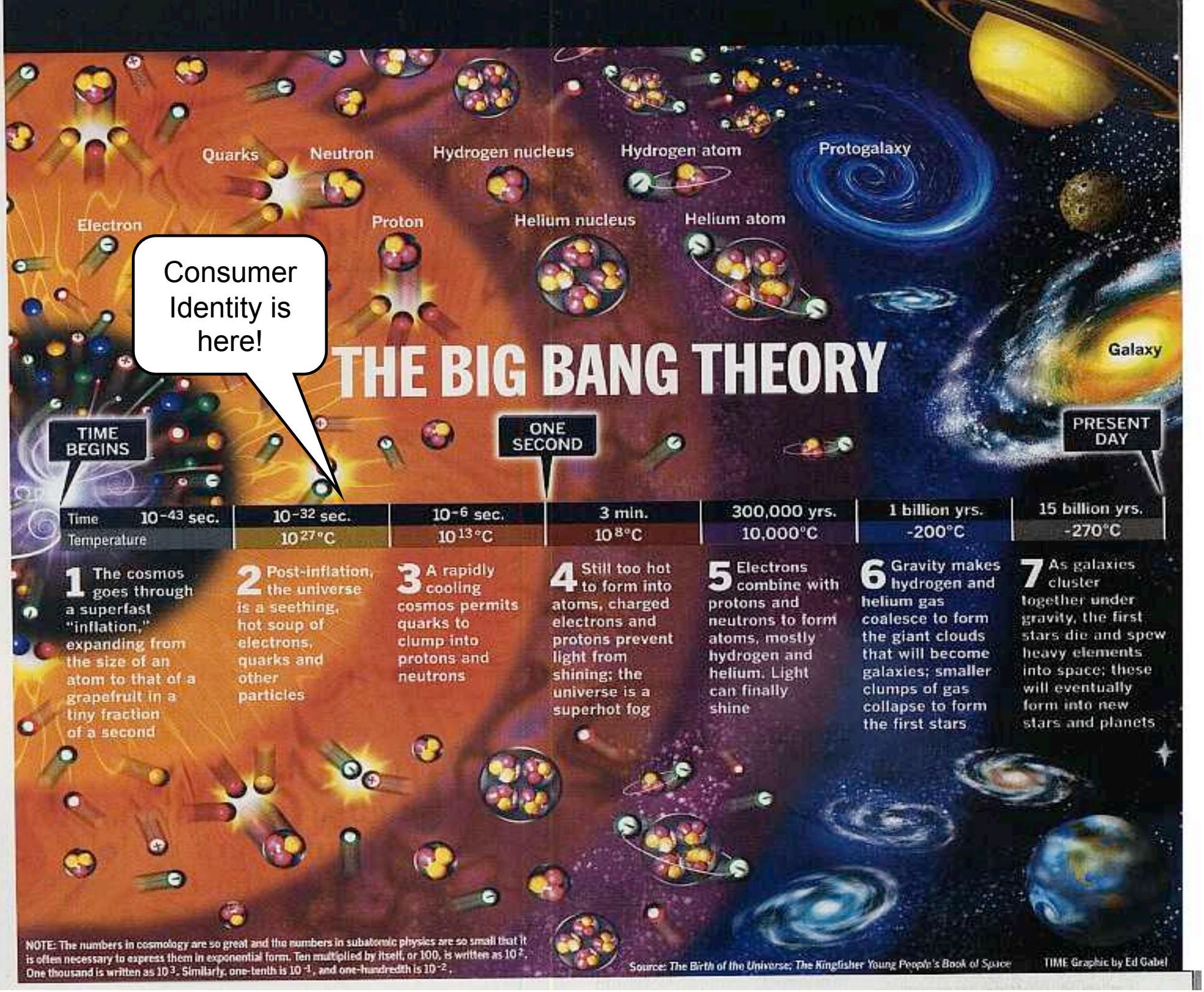
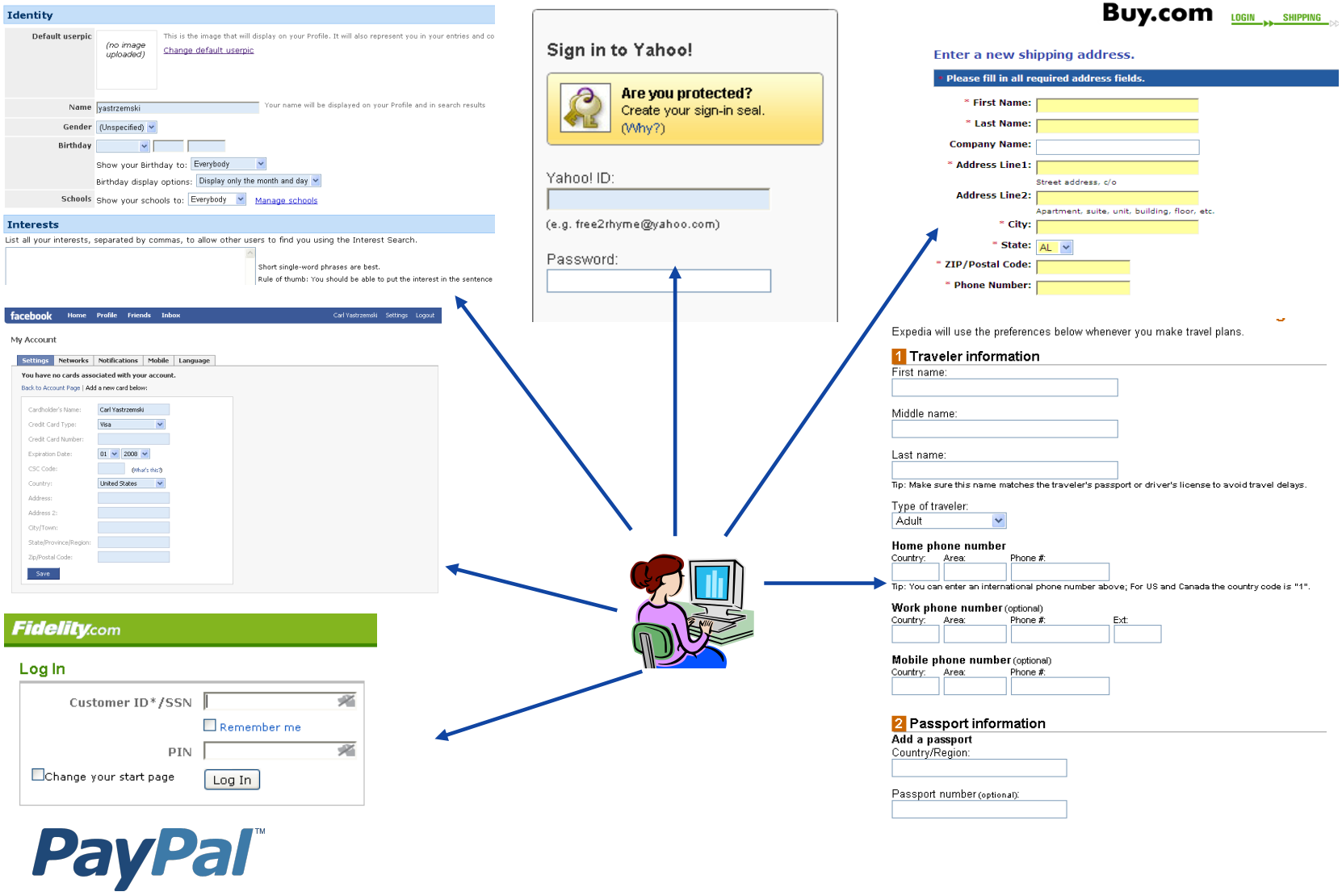
Identity Assurance and your Real World Identity

Andrew Nash
Senior Director of Identity Services


Quarks
Neutron
Hydrogen nucleus
Hydrogen atom
Protogalaxy
Electron
Proton
Helium nucleus
Helium atom
Consumer Identity is here!
THE BIG BANG THEORY
Galaxy
TIME BEGINS
ONE SECOND
PRESENT DAY
Time 10-43 sec. | 10-32 sec. | 10-6 sec. | 3 min. | 300,000 yrs. | 1 billion yrs. | 15 billion yrs.
Temperature 10 27 °C | 10 13 °C | 10 8 °C | 10,000°C | -200°C | -270°C
1 The cosmos goes through a superfast "inflation," expanding from the size of an atom to that of a grapefruit in a tiny fraction of a second
2 Post-inflation, the universe is a seething, hot soup of electrons, quarks and other particles
3 A rapidly cooling cosmos permits quarks to clump into protons and neutrons
4 Still too hot to form into atoms, charged electrons and protons prevent light from shining; the universe is a superhot fog
5 Electrons combine with protons and neutrons to form atoms, mostly hydrogen and helium. Light can finally shine
6 Gravity makes hydrogen and helium gas coalesce to form the giant clouds that will become galaxies; smaller clumps of gas collapse to form the first stars
7 As galaxies cluster together under gravity, the first stars die and spew heavy elements into space; these will eventually form into new stars and planets
NOTE: The numbers in cosmology are so great and the numbers in subatomic physics are so small that it is often necessary to express them in exponential form. Ten multiplied by itself, or 100, is written as 10 2. One thousand is written as 10 3. Similarly, one-tenth is 10 -1, and one-hundredth is 10 -2.
Source: The Birth of the Universe: The Kingfisher Young People's Book of Space
TIME Graphic by Ed Gabel

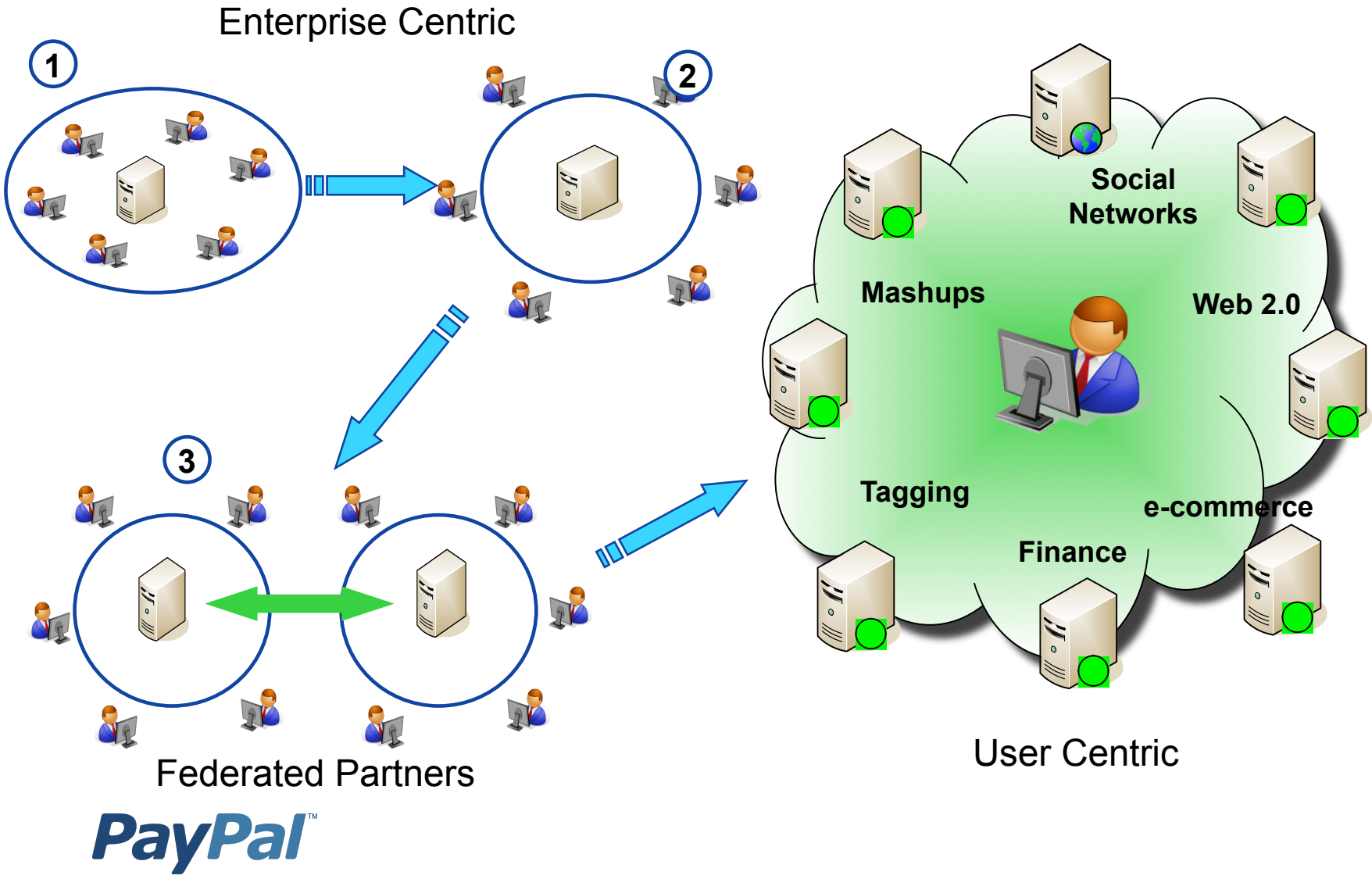
Internet Consumer Identity …Yesterday?

Consumer Internet interactions are repetitive, frustrating and littered with outdated info

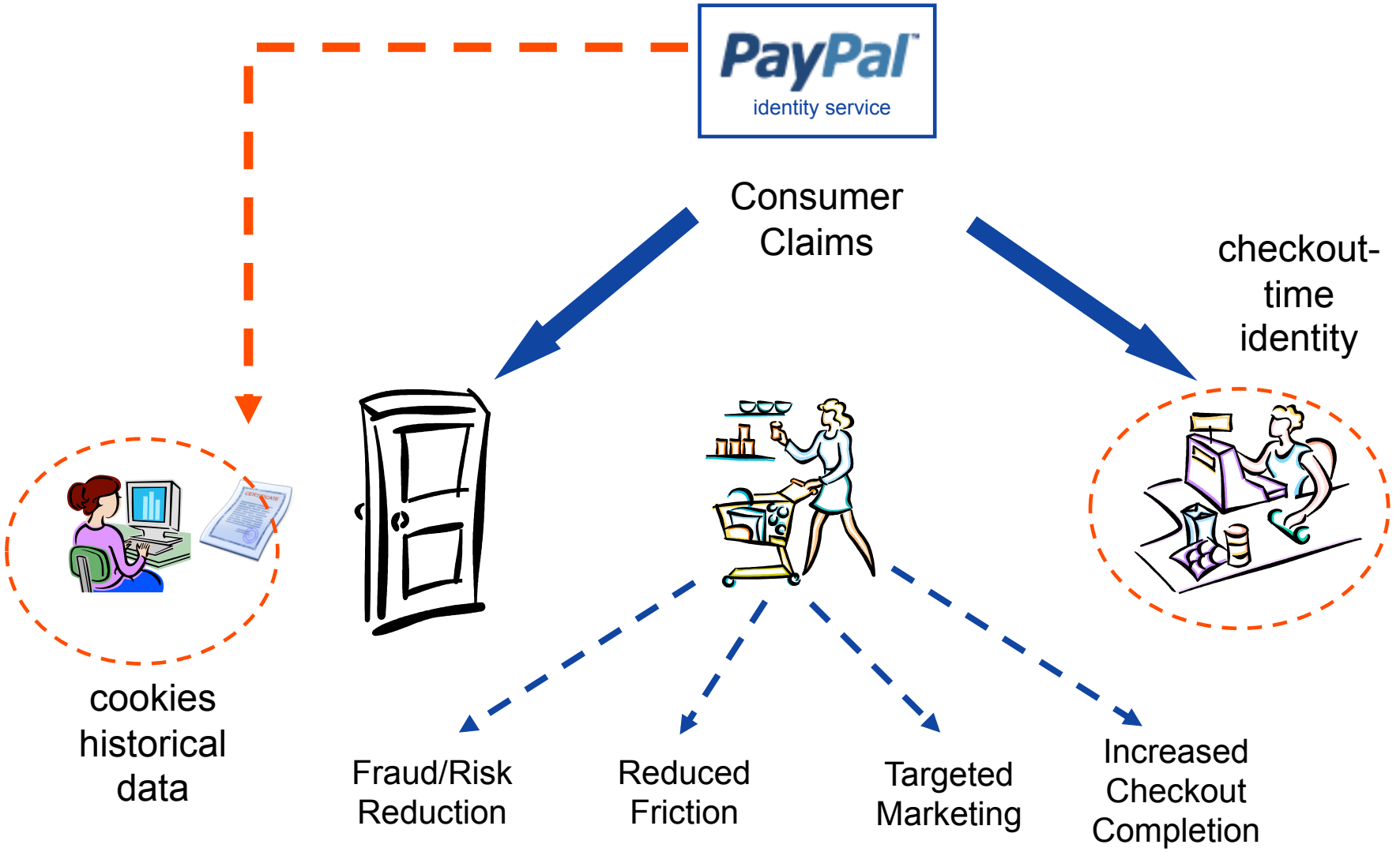


Consumer Trust and Safety

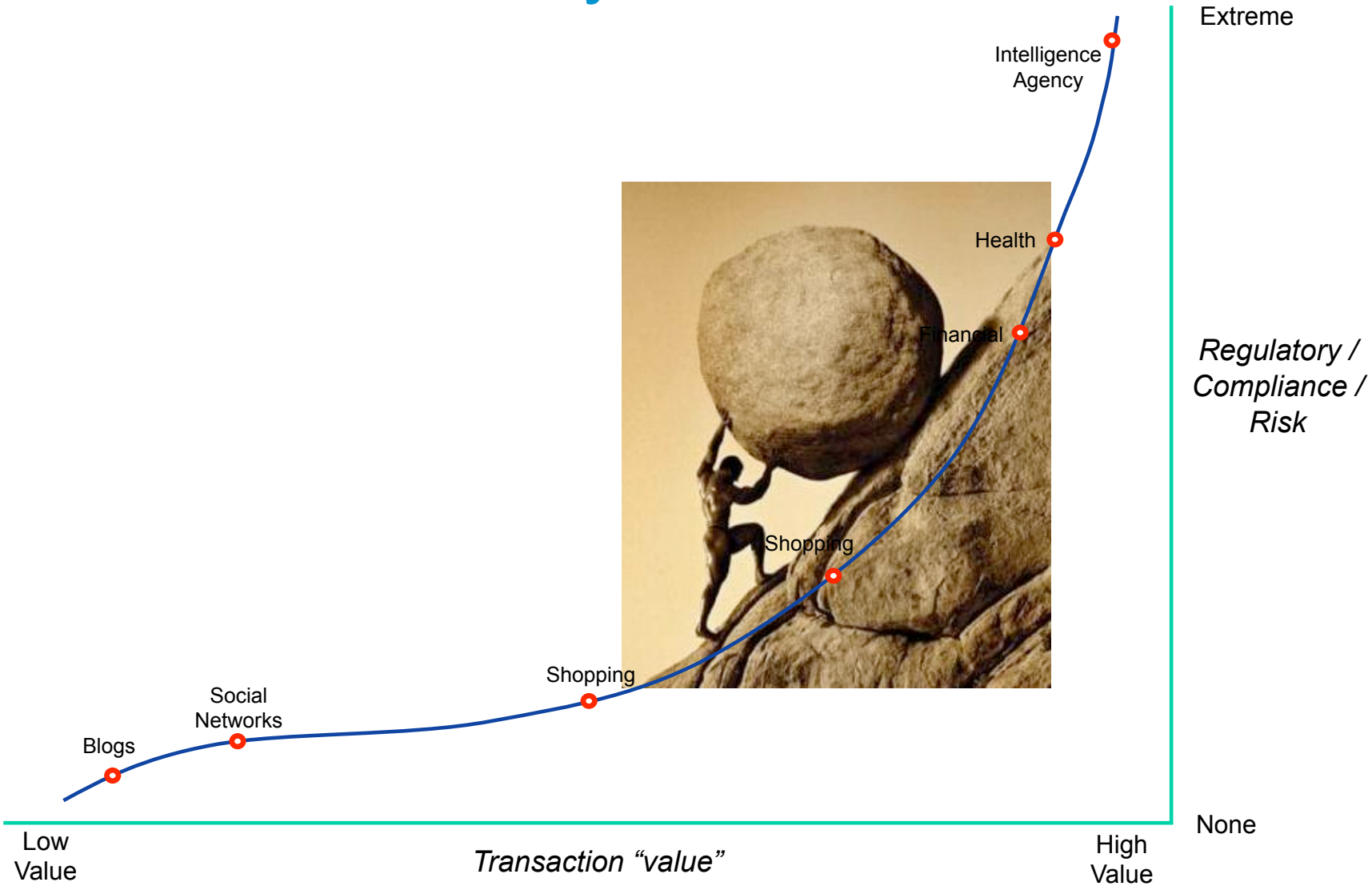
Identity Evolution
Finally Addressing the Consumer



Transactional Opportunity



The Identity Trust Gradient



PayPal™

Identity Assurance Frameworks

- Kantara (and others)
  - Framework supporting mutual acceptance, validation and lifecycle maintenance across identity federations
- It consists of 4 parts:
  - Assurance Levels
  - Service Assessment Criteria
  - Accreditation and Certification Model
  - Business Rules

PayPal™

US Federal Govt Assurance Levels

Assurance Level	Example	Assessment Criteria – Organization	Assessment Criteria – Identity Proofing	Assessment Criteria –
AL 1	Registration to a news website	Minimal Organizational criteria	Minimal criteria - Self assertion	
AL 2	Change of address of record by beneficiary	Moderate organizational criteria	Moderate criteria - Attestation of Govt. ID	ntrol of token through authentication protocol
AL 3	Access to an online brokerage account	Stringent organizational criteria	Stringent criteria – stronger attestation and verification of records	Multi-factor auth; Cryptographic protocol; “soft”, “hard”, or “OTP” tokens
AL 4	Dispensation of a controlled drug or $1mm bank wire	Stringent organizational criteria	More stringent criteria – stronger attestation and verification	Multi-factor auth w/hard tokens only; crypto protocol w/keys bound to auth process

Face-to-Face or Multiple Forms of Govt Id

PayPal™

So how is it, that…

- Anonymity with user attributes is acceptable?
  - One time credit card #
    + shipping address
    = product shipment

PayPal™

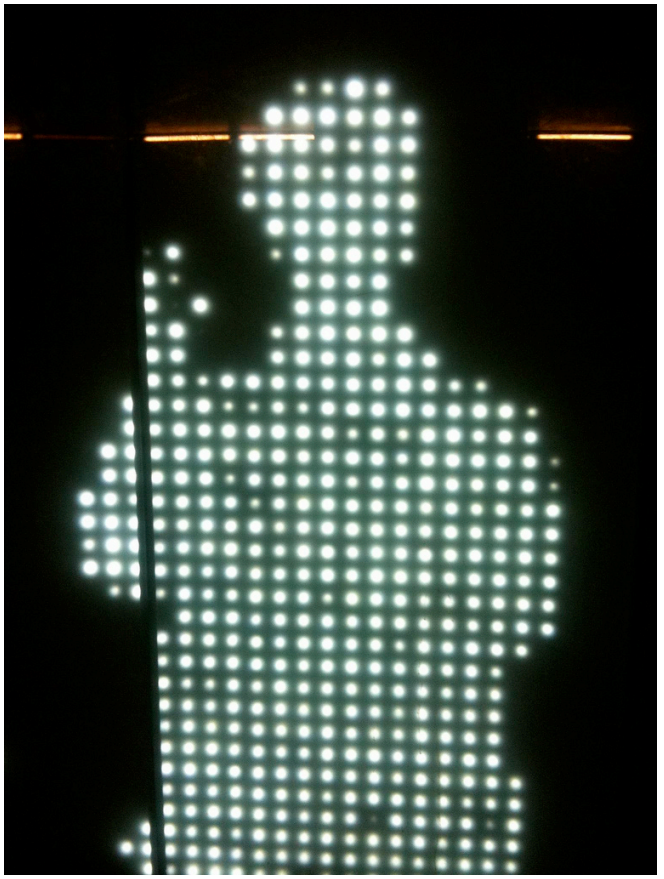
So how is it, that…

- You can perform a transaction with a high level of assured identity but low authentication
  - E-commerce
  - Library borrowing

PayPal™

So how is it…

- A digital representation of me is sufficient in many (most?) cases as opposed to my real world identity



- Additional conversation at:

http://www.xmlgrrl.com/blog/2009/12/31/how-to-rest-assured/

http://connectid.blogspot.com/2010/01/taxonomy-of-federated-applications.html

PayPal™

Well for a start …

- There should be a lot more levels between AL1 and AL2
- Pseudo-anonymity should have much broader acceptance (maybe at all levels)
- In broad e-commerce transactional domains a level 1.x may be the 80% case
- Even government e-commerce transactions probably don't have to know who you are

PayPal™

But maybe mostly because …

- The model fails to account for risk based processing
- Financial institutions and most commerce sites apply a set of risk based evaluation rules

PayPal™

But maybe mostly because …

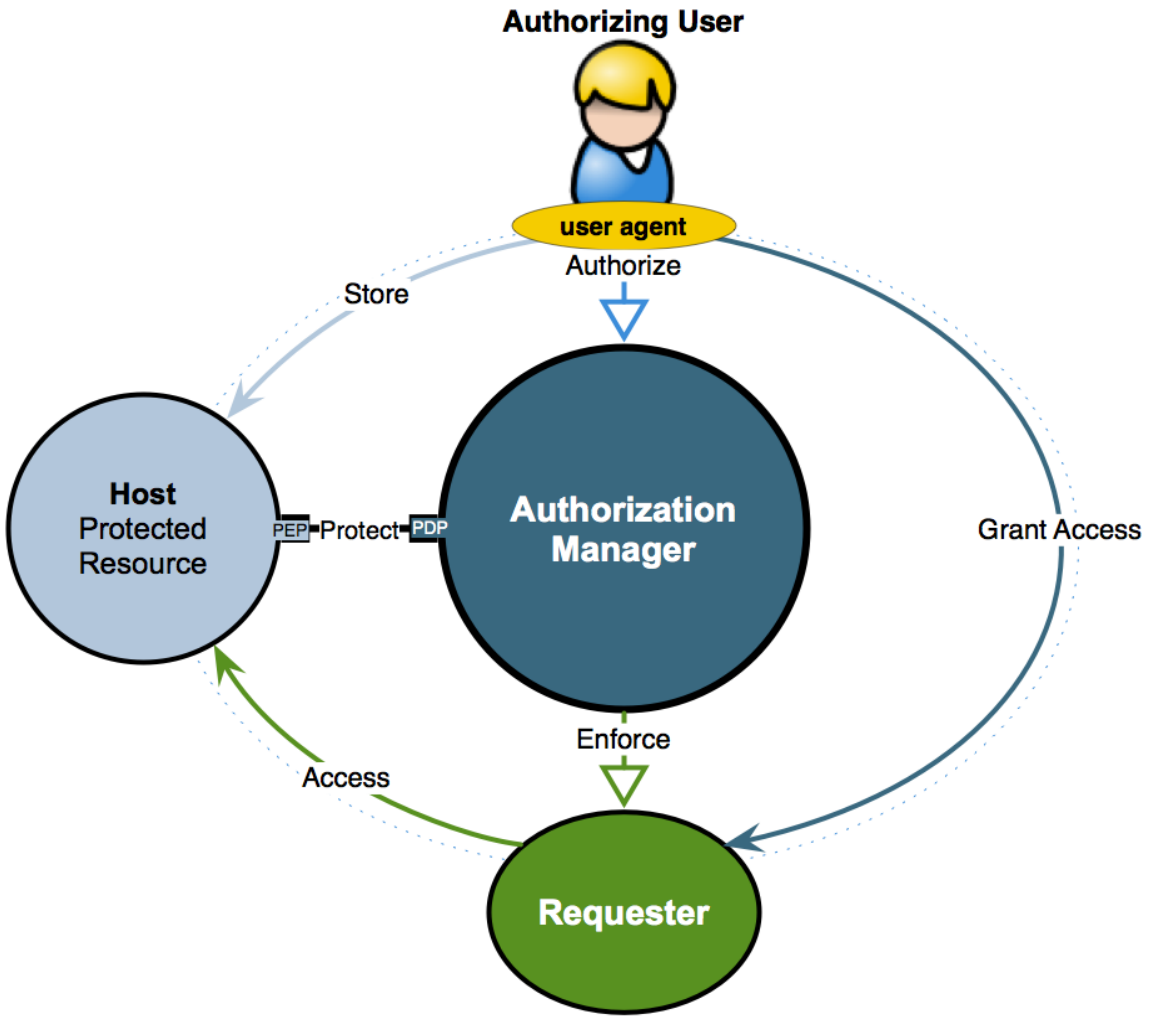
- Unlike NIST, risk based systems are not a one time identity proofing exercise
- Continual verification of identity “goodness”
  - Context, transaction history, behavior, …
- Enhancement to authentication
  - Triggers for step-up authentication

PayPal™

US Federal Privacy Policy

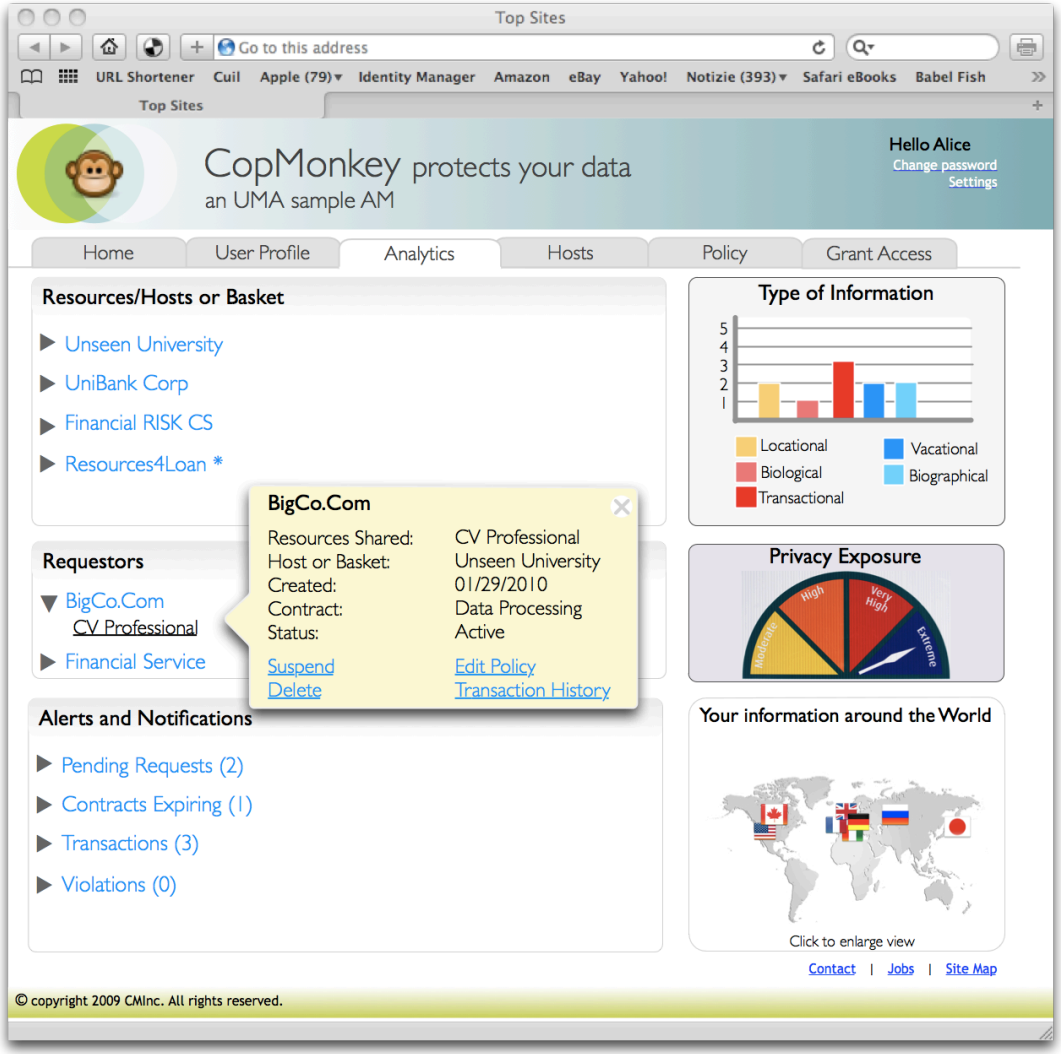
- Informed Consent
  - Define default information to be released to RPs
  - Should provide ability to deny release of certain attributes
- Abstract Identifier
  - Where PII not required
- Minimal Transmission
  - No more attrib than required shared
- Activity Tracking
  - Not disclosed to other parties

User Managed Access



PayPal™ http://kantarainitiative.org/confluence/display/uma/UMA+Explained

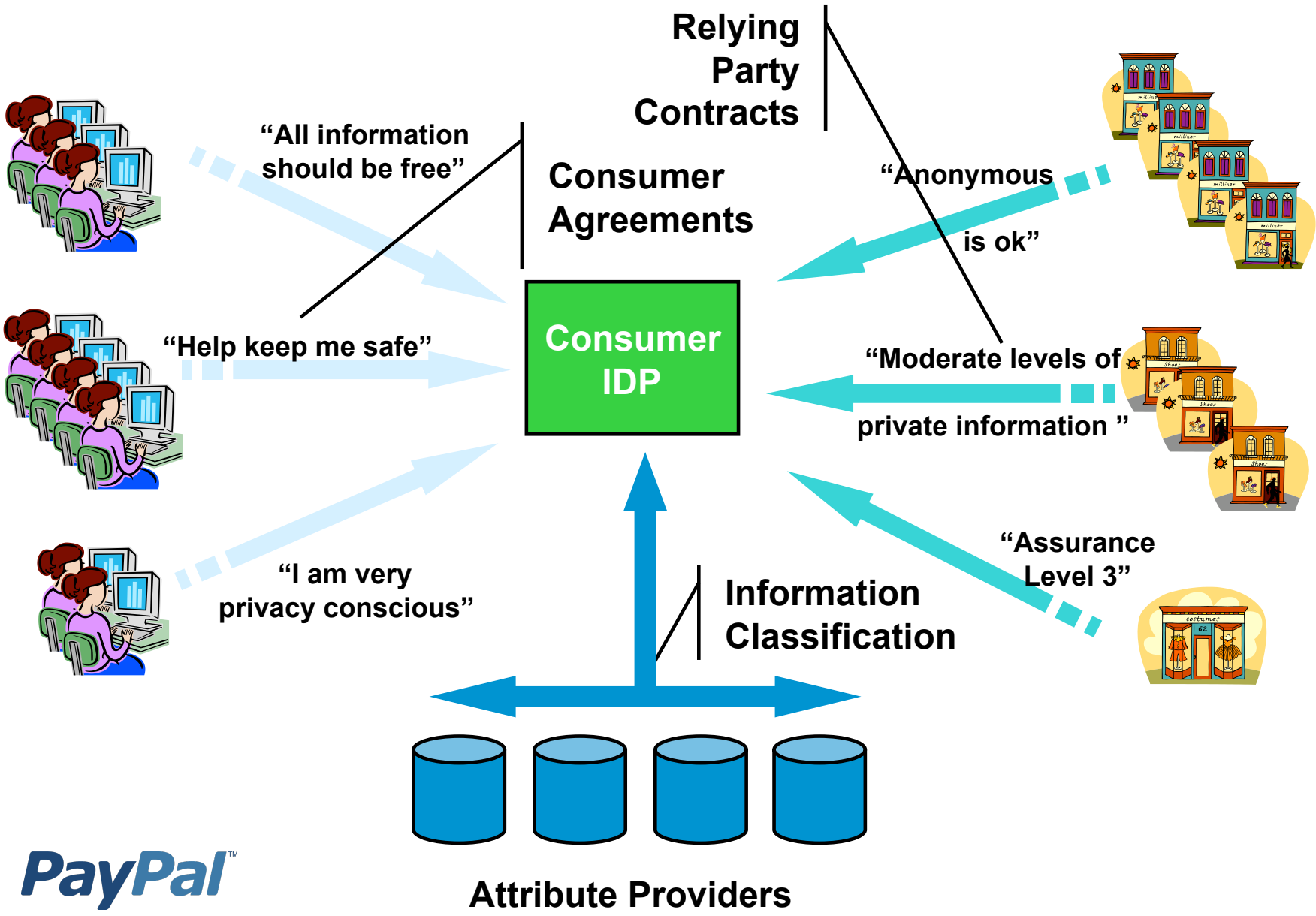
UMA Dashboard



PayPal™

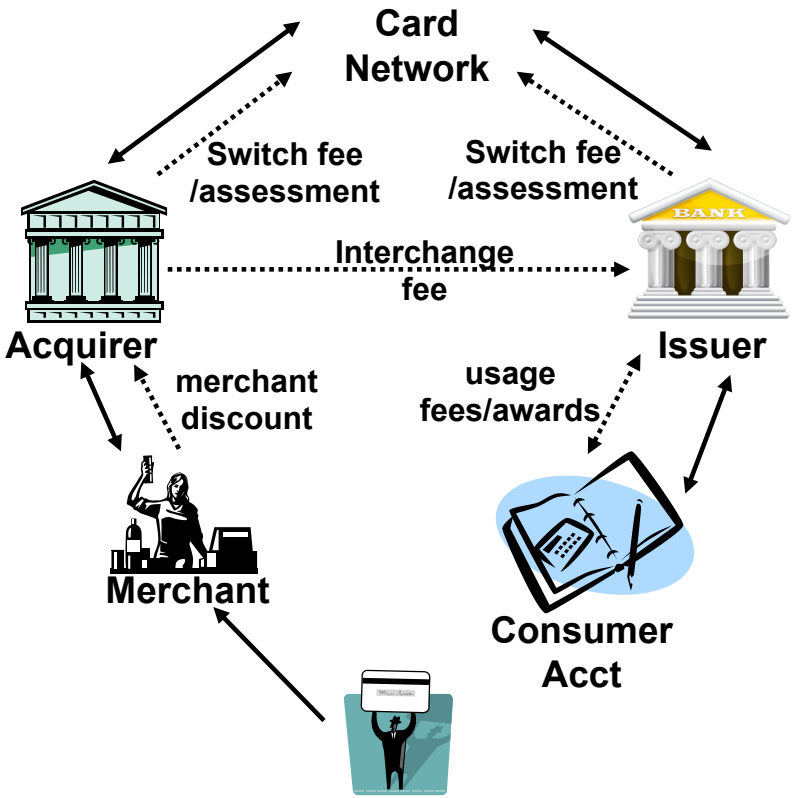
http://kantarainitiative.org/confluence/display/uma/User+Experience

Role of IDP?


Relying Party Contracts
Consumer Agreements
"All information should be free"
"Help keep me safe"
"I am very privacy conscious"
"Anonymous is ok"
"Moderate levels of private information "
"Assurance Level 3"
Consumer IDP
Information Classification
Attribute Providers
PayPal™

Credit Card Analog

- Credit cards evolved a similar if more complex ecosystem
- Consumer and Merchant agreements with penalties
- Caveat Emptor
  - Credit card system is in a steady state
  - VERY different world during startup phase
  - Features now available were not economically viable during the equivalent credit card big bang



PayPal™

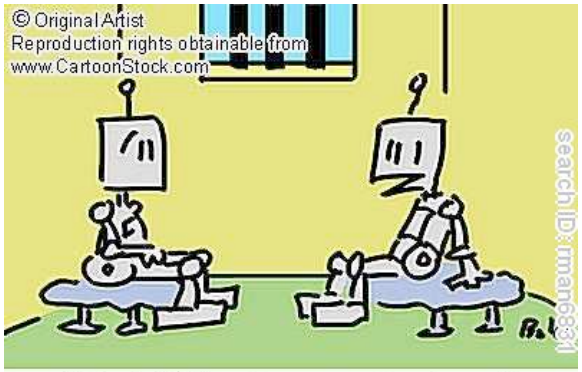
Consumer IDP as Consumer Advocate

- Consumer IDP must be focused on:
  - The success of their users
  - Privacy and Control
  - Usability
- Anonymity – the cut case
- Consumer Control / Permission
  - Tools and protocols necessary but not sufficient condition
  - Consumer information classification
    - What does the consumer think is sensitive?
    - What are the trigger conditions?
- Notification
  - Exception reporting in human terms
- Auditing
  - “Just where did I go last week…?”

PayPal™

The Three Laws of Consumer IDP's???

1. An IDP may not injure a consumer, or through inaction, allow a consumer to come to harm.
2. An IDP must obey orders given by consumers, except where such orders would conflict with the First Law.
3. An IDP must protect its own existence as long as such protection does not conflict with the First or Second Law.



"No kidding? — you broke all *three* laws of robotics?"

PayPal™

Unpaid Plug

PayPal™


PayPal™


PayPal™