RSAConference2015
San Francisco | April 20-24 | Moscone Center

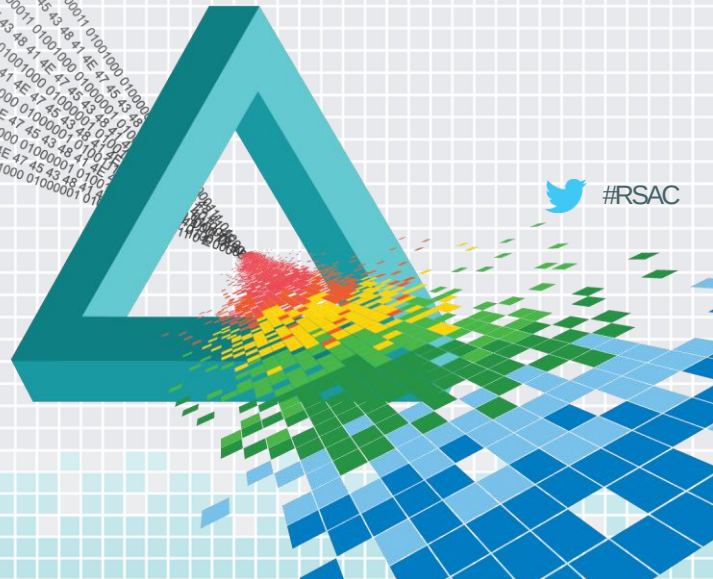
SESSION ID: ECO-R01

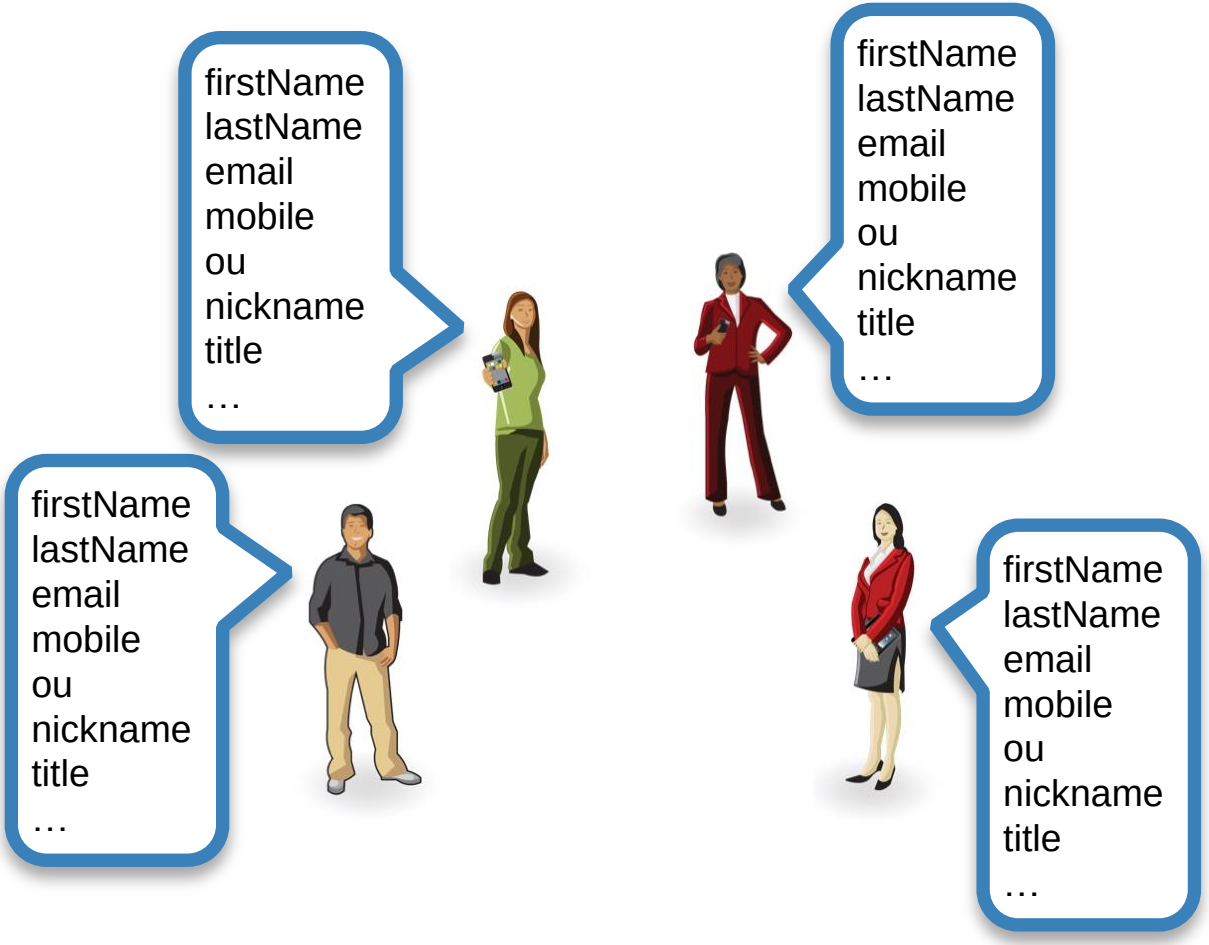
On the Care and Feeding of Human and Device Relationships

Ian Glazer
Senior Director, Identity
Salesforce
@iglazer

Eve Maler
VP of Innovation & Emerging Technology
ForgeRock
@xmlgrrl

Killing Identity and Access Management: The Road to Identity Relationship Management




firstName
lastName
email
mobile
ou
nickname
title
…
firstName
lastName
email
mobile
ou
nickname
title
…
firstName
lastName
email
mobile
ou
nickname
title
…
firstName
lastName
email
mobile
ou
nickname
title
…

Reasonably large number of identities with a reasonable number of attributes

deviceID
firmware

deviceID
firmware

deviceID
firmware

deviceID
firmware









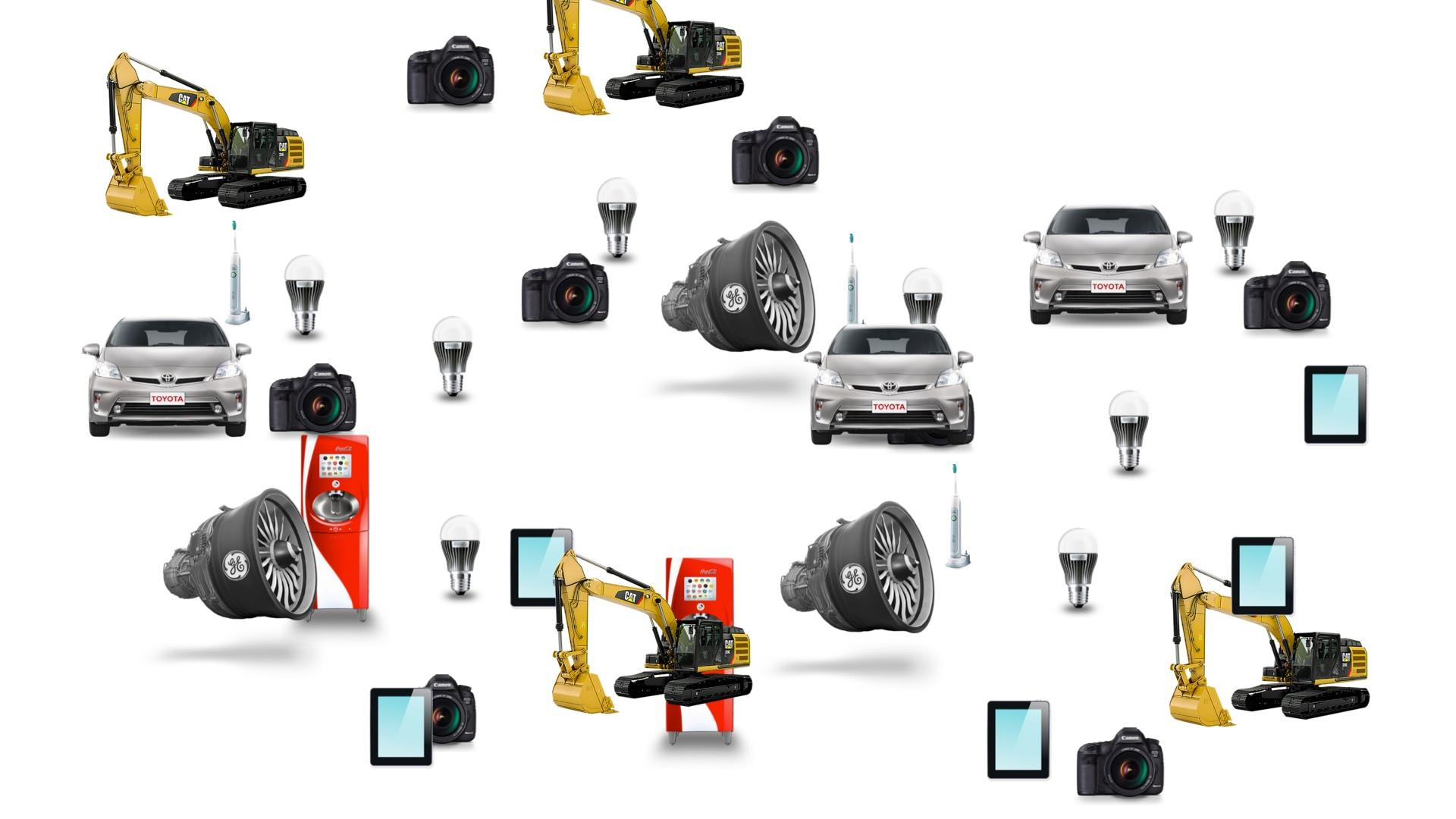


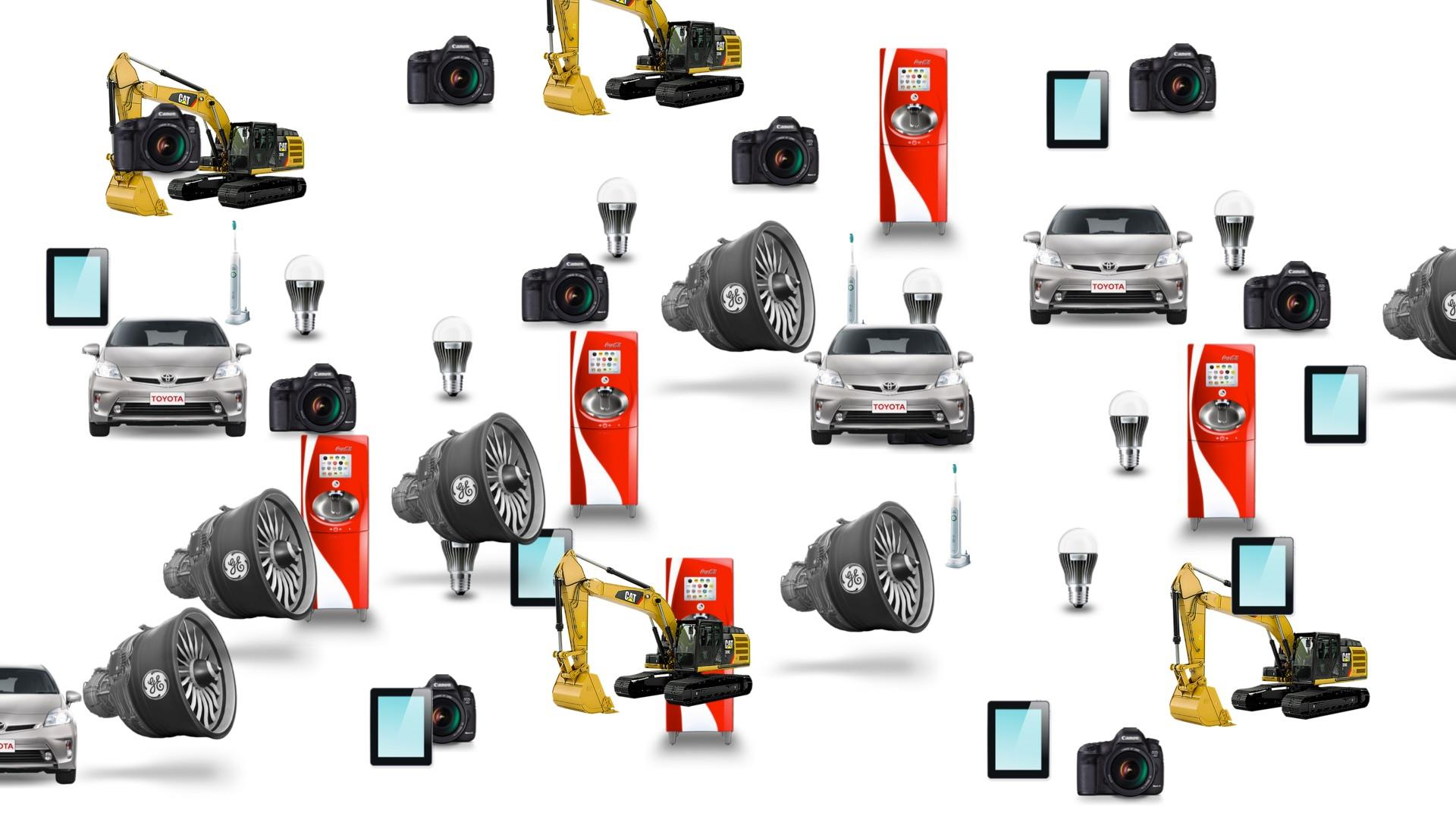


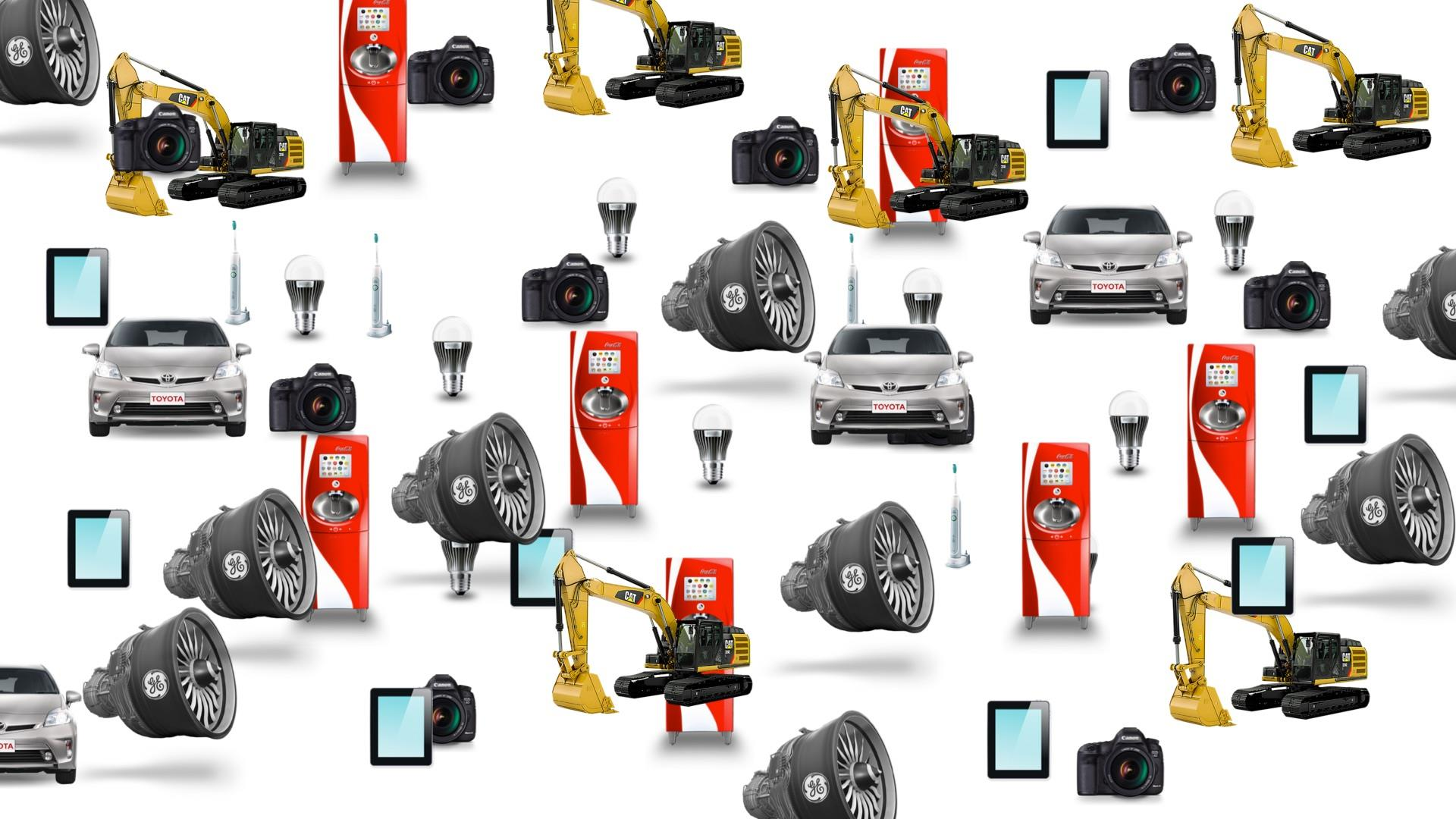




CAT
CAT
CAT


CAT
TOYOTA


CAT
TOYOTA


CAT
TOYOTA

Unreasonably large number of identities with a few attributes

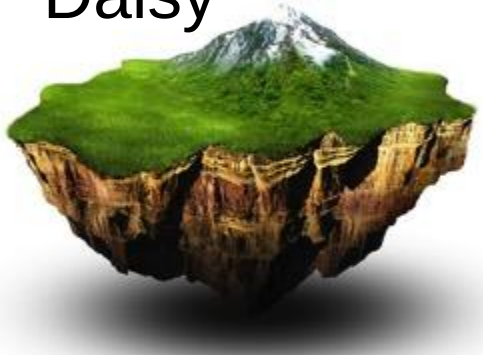
```
mysql> select * from users;
+----+--------+--------+---------------------+
| id | f_name | l_name | email               |
+----+--------+--------+---------------------+
|  1 | Bobby  | Tables | lil_bob@xkcd.com    |
|  2 | Scott  | Tiger  | housecat@oracle.com |
|  3 | Babs   | Jensen | daisypop89@gmail.com |
+----+--------+--------+---------------------+
3 rows in set (0.00 sec)
```

Bobby

Scott

Us

Daisy



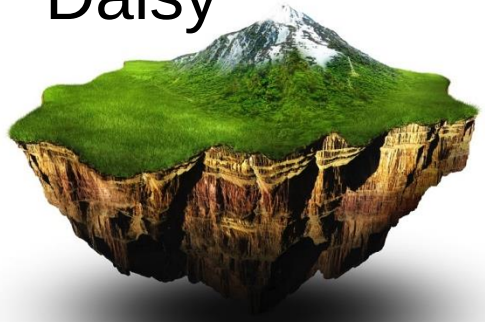
dc=com
 |
 dc=example
  |
  ou=north
   |
   cn=Bobby Tables, mail=lil_bob@xkcd.com
  |
  ou=west
   |
   cn=Daisy Jensen, mail=daisypop89@gmail.com
   cn=Scott Tiger, mail=housecat@oracle.com

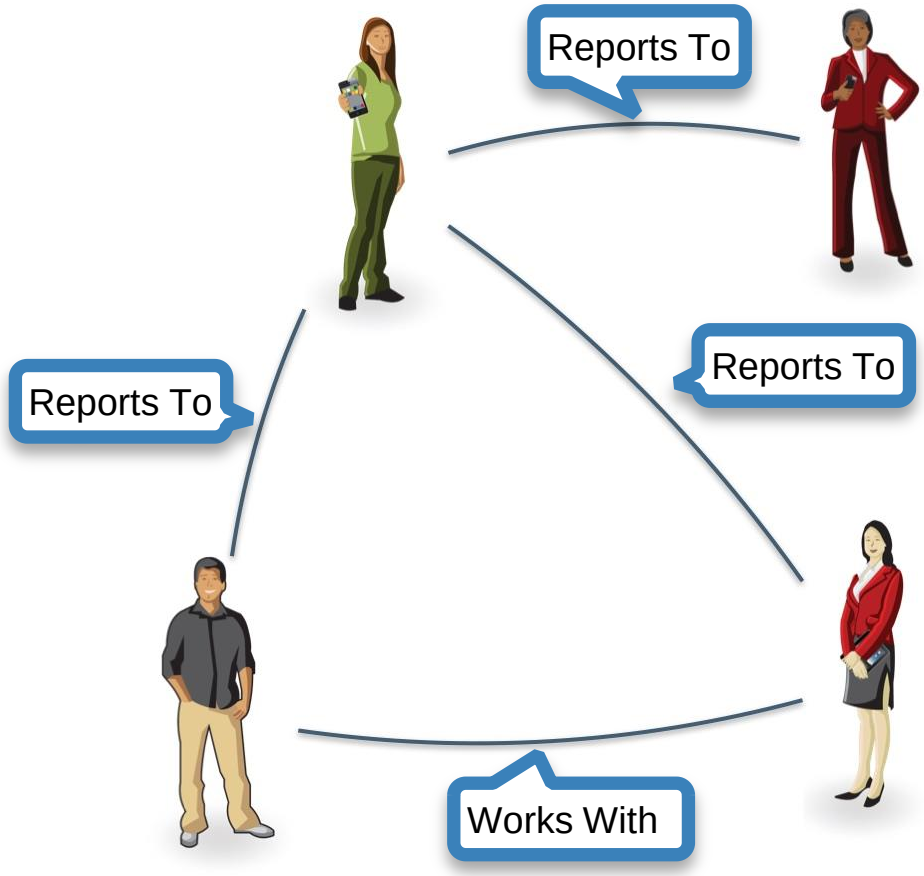
Bobby

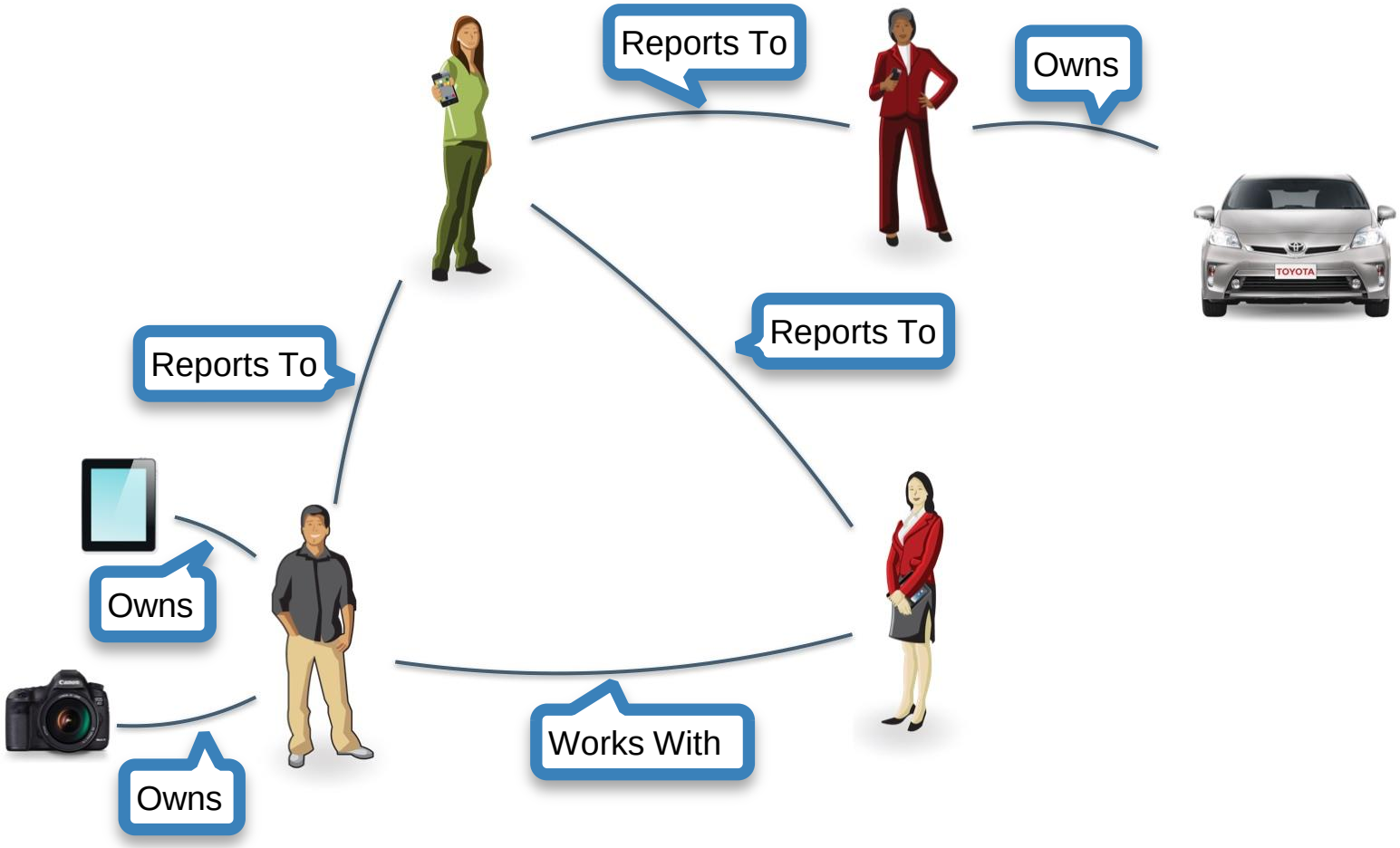
Scott

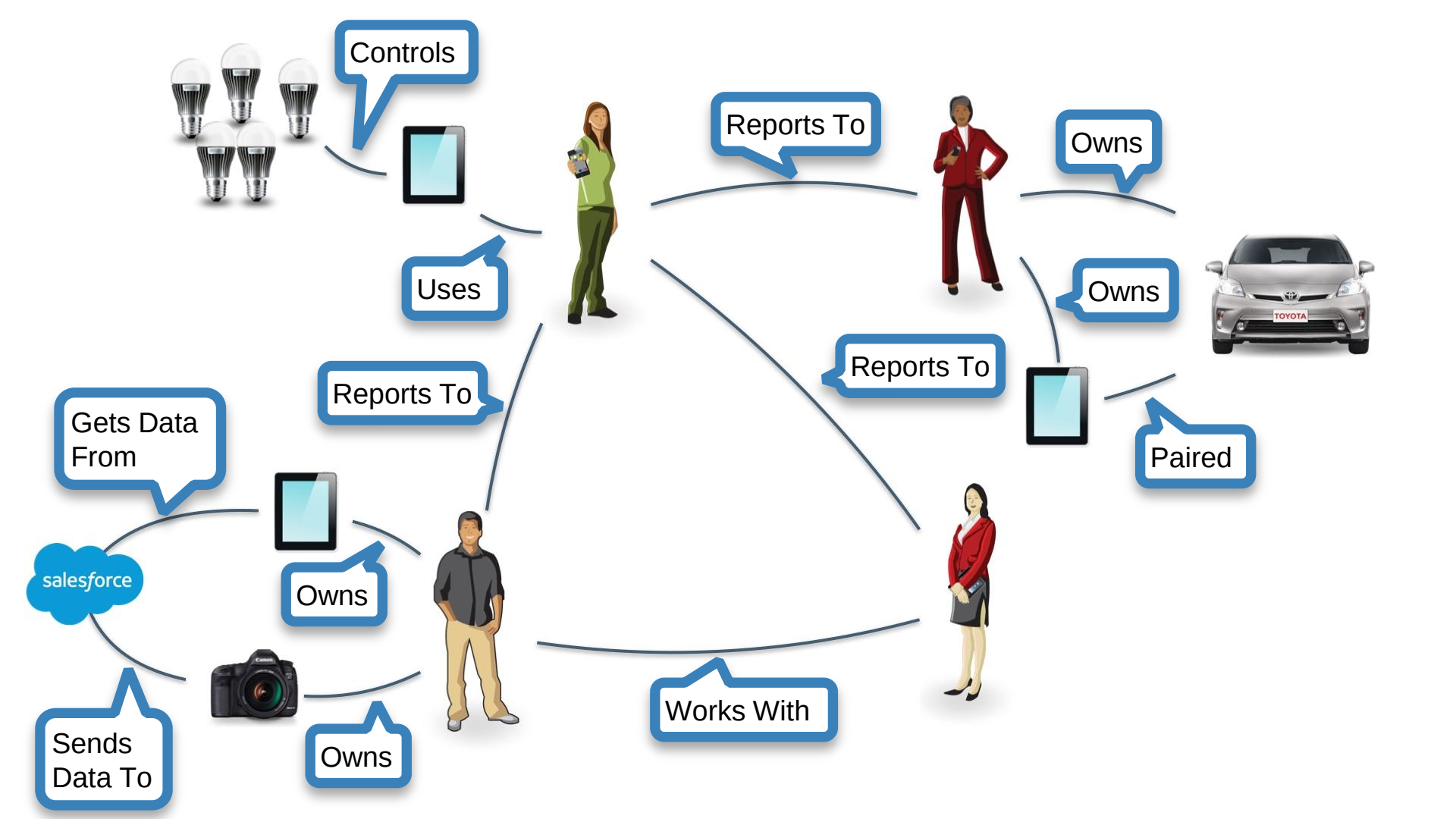
Us

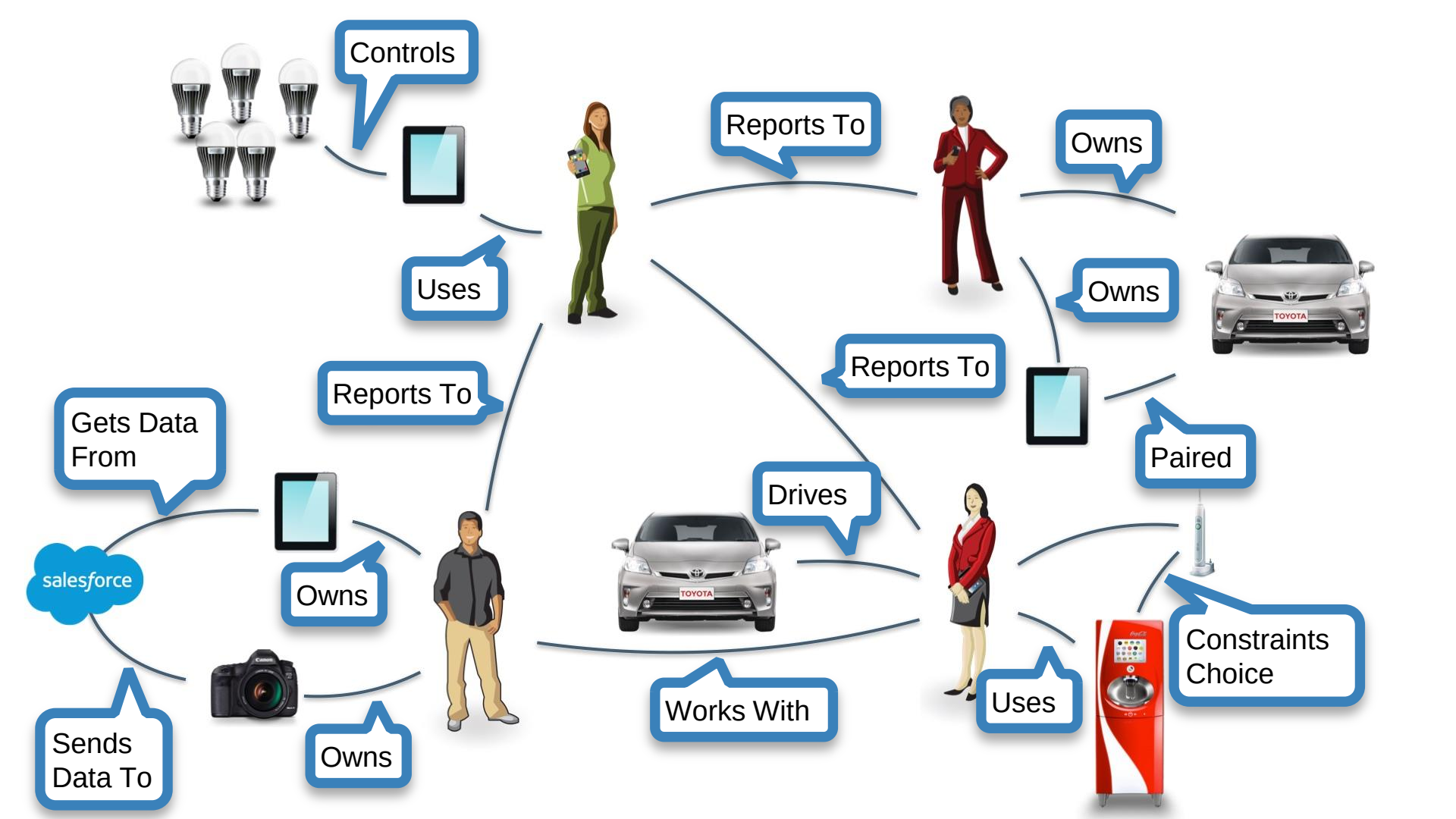
Daisy

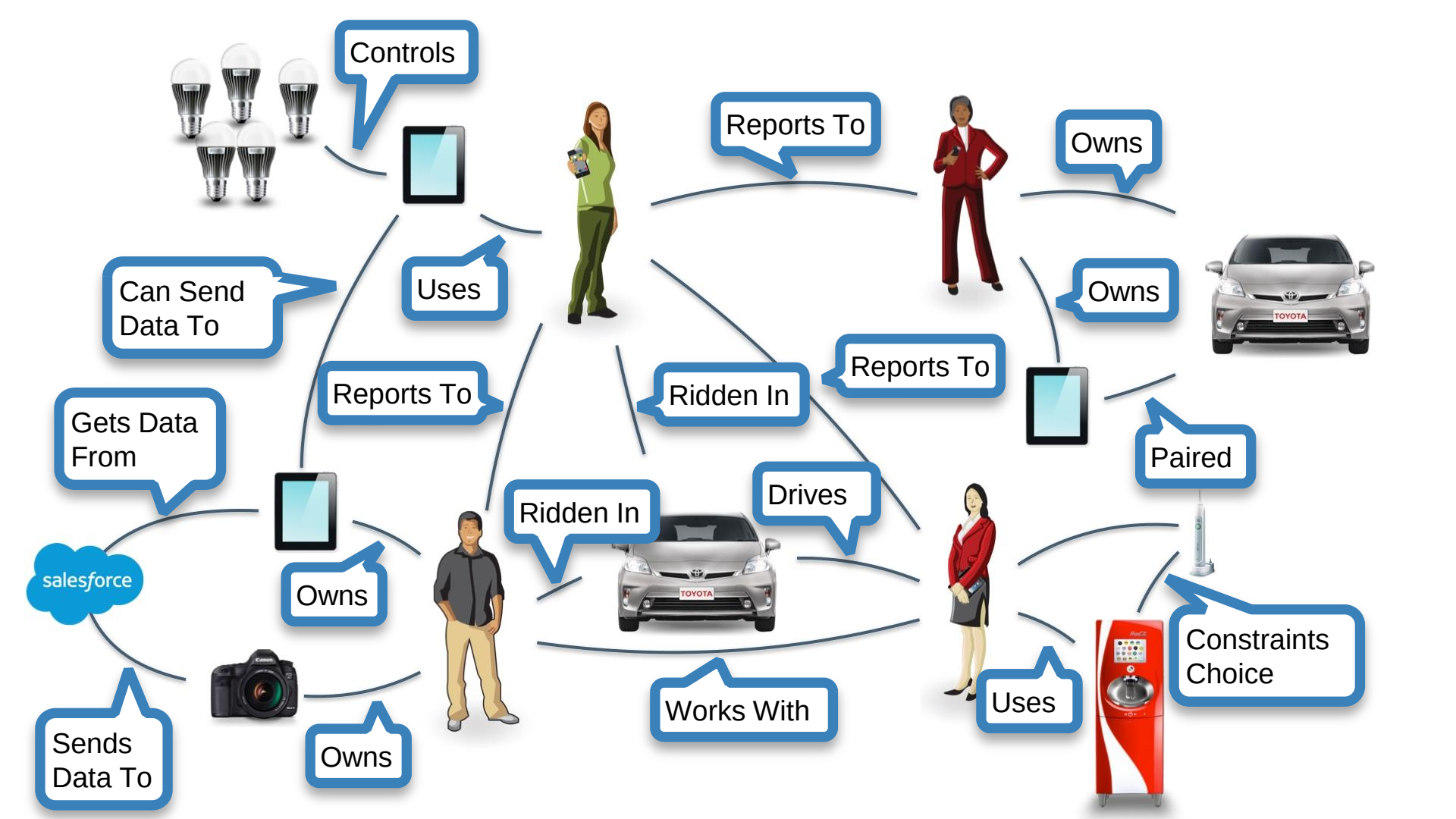


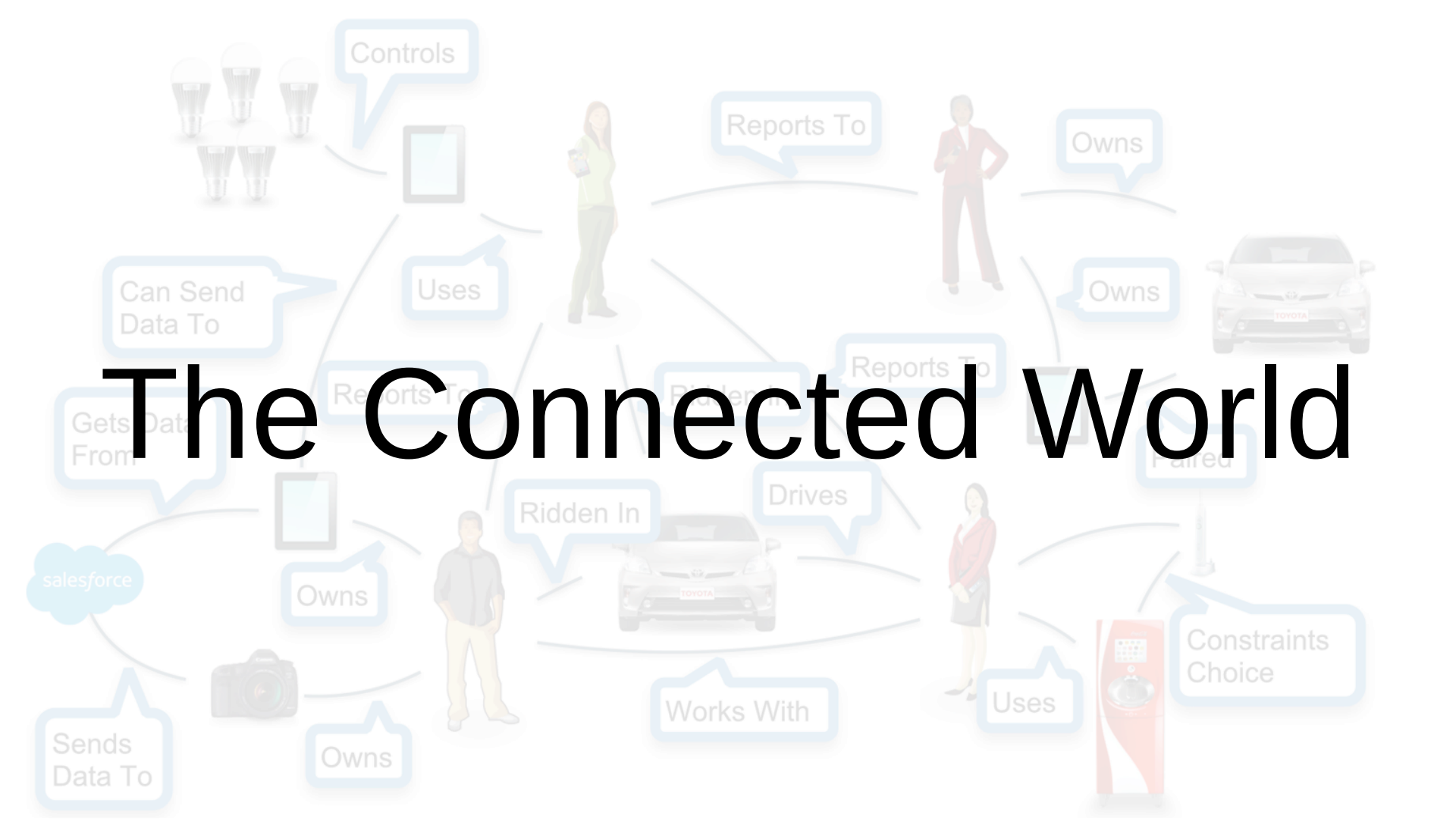

Reports To
Reports To
Reports To
Works With


Reports To
Owns
Reports To
Reports To
Owns
Owns
Works With


Controls
Uses
Reports To
Owns
Owns
Reports To
Paired
Reports To
Gets Data From
Owns
Sends Data To
Owns
Works With
salesforce
TOYOTA


Controls
Uses
Reports To
Owns
Owns
Reports To
Reports To
Paired
Drives
Constraints
Choice
Uses
Works With
Gets Data
From
Owns
Sends
Data To
Owns
salesforce
TOYOTA
TOYOTA


Controls
Reports To
Owns
Can Send Data To
Uses
Owns
Reports To
Ridden In
Reports To
Gets Data From
Paired
Drives
Ridden In
Owns
Constraints
Choice
Works With
Uses
Sends Data To
Owns
salesforce
TOYOTA
TOYOTA



The Connected World

Principles of Identity Relationship Management

- Scalable
- Acknowledgeable & Provable
- Actionable & Constrainable
- Immutable & Transferable
- Activatable & Revocable

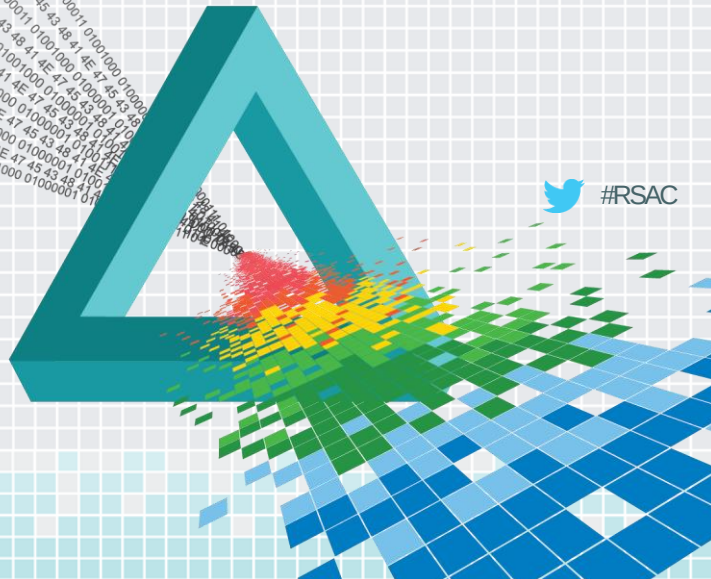

kantara
INITIATIVE
TM

Do we have to throw the baby out with the bath water? Can’t we use the techniques we’ve already learned?

RSAConference2015

San Francisco | April 20-24 | Moscone Center

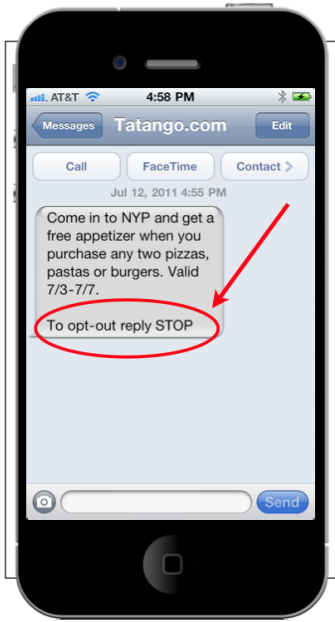
Old-Style Consent Is Broken For Supporting Relationships



#RSAC

about:blank

about:blank



To Opt-Out Reply STOP

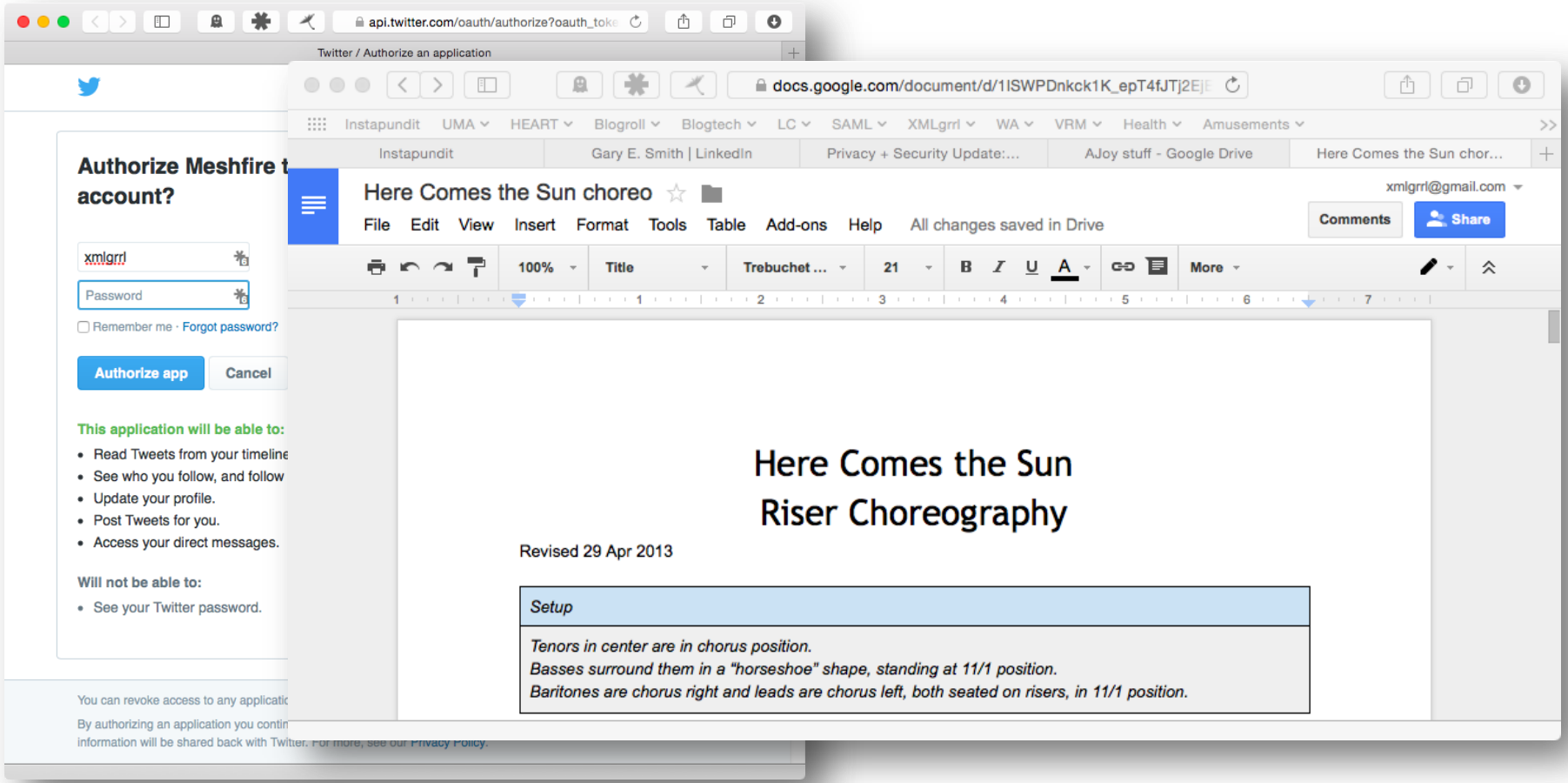
Email:

☑ Newsletter: Keep me up to date with [redacted] news, software updates and the latest information on products and services.

☐ I agree to the Terms and Conditions (Required - See Link Below).

Continue

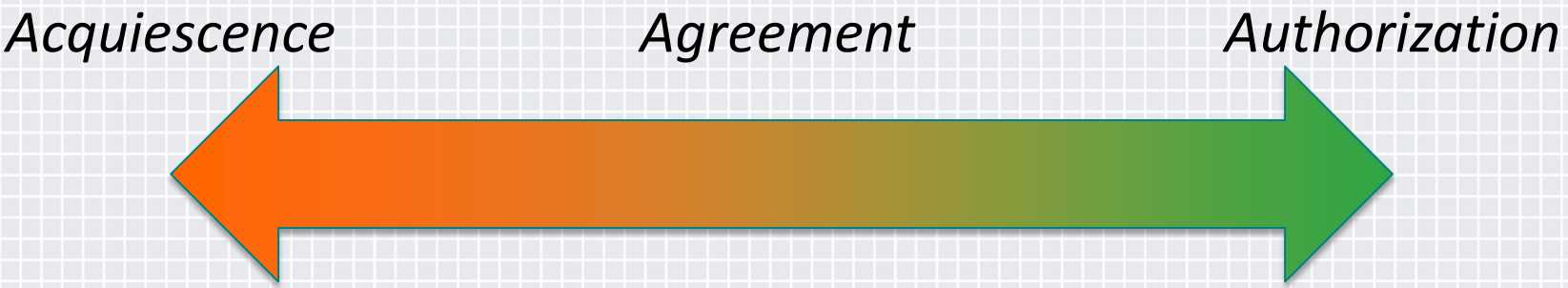
Terms and Conditions [redacted] Privacy Policy


api.twitter.com/oauth/authorize?oauth_toke
Twitter / Authorize an application
Authorize Meshfire t
account?
xmlgrrl
Password
Remember me · Forgot password?
Authorize app
Cancel
This application will be able to:
Read Tweets from your timeline
See who you follow, and follow
Update your profile.
Post Tweets for you.
Access your direct messages.
Will not be able to:
See your Twitter password.
You can revoke access to any applicatio
By authorizing an application you contin
information will be shared back with Twitter. For more, see our Privacy Policy.
docs.google.com/document/d/1ISWPDnkck1K_epT4fJTj2E
Instapundit
UMA
HEART
Blogroll
Blogtech
LC
SAML
XMLgrrl
WA
VRM
Health
Amusements
Instapundit
Gary E. Smith | LinkedIn
Privacy + Security Update:...
AJoy stuff - Google Drive
Here Comes the Sun chor...
Here Comes the Sun choreo
xmlgrrl@gmail.com
File
Edit
View
Insert
Format
Tools
Table
Add-ons
Help
All changes saved in Drive
Comments
Share
100%
Title
Trebuchet ...
21
More
Here Comes the Sun
Riser Choreography
Revised 29 Apr 2013
Setup
Tenors in center are in chorus position.
Basses surround them in a "horseshoe" shape, standing at 11/1 position.
Baritones are chorus right and leads are chorus left, both seated on risers, in 11/1 position.

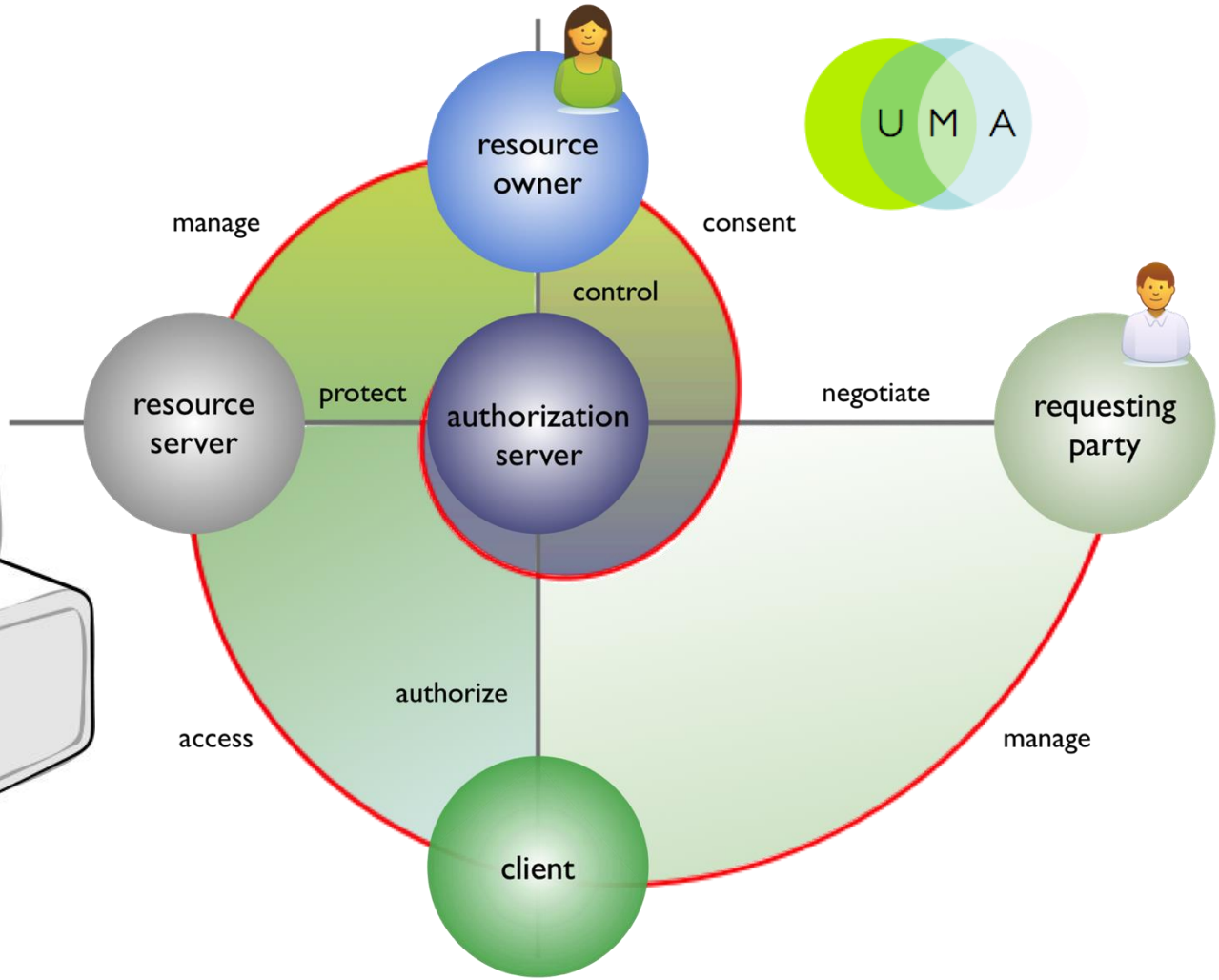

Tom kg
54.3
Tom kg
54.3
Withings

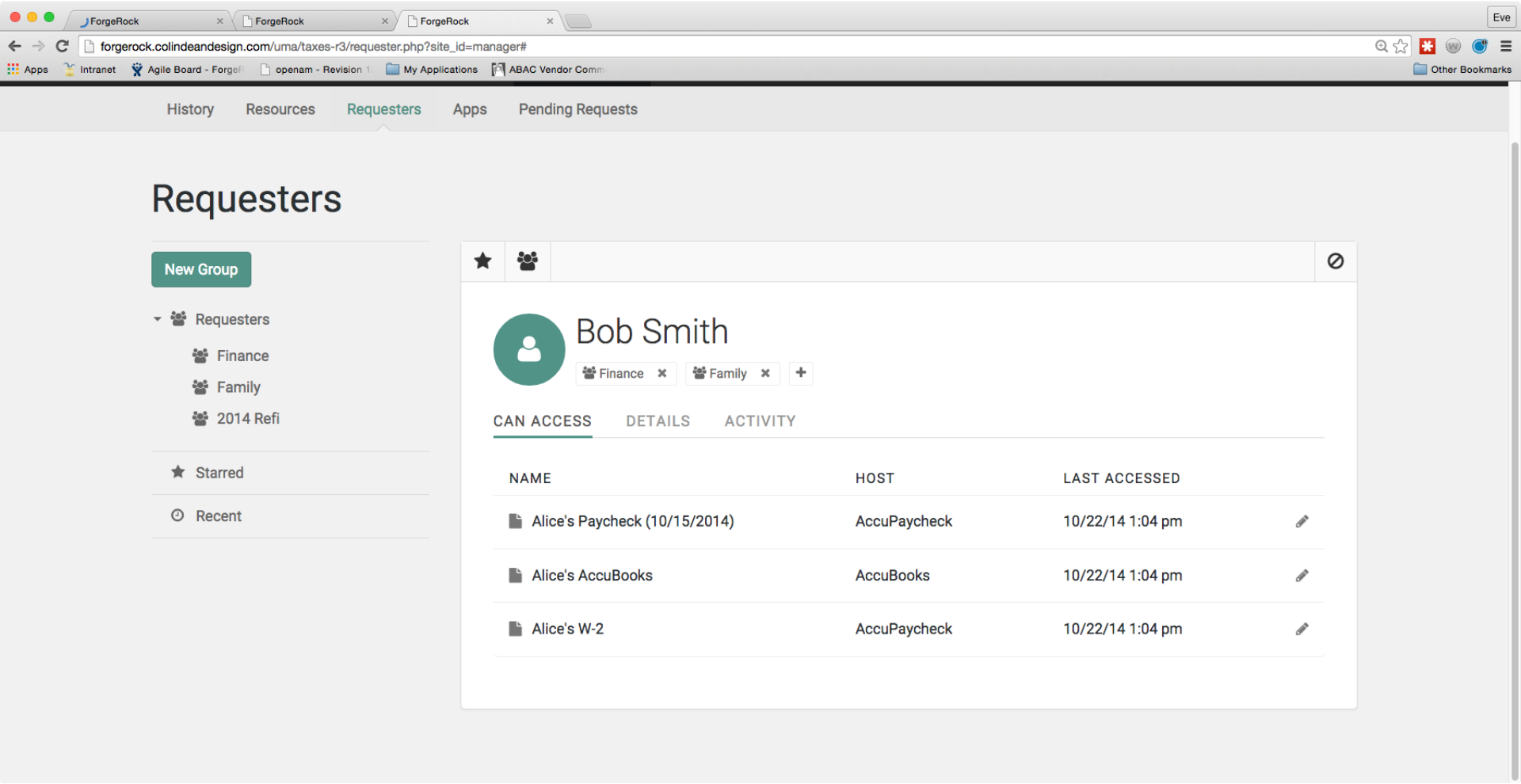

Tom kg
54.3
Share
Tom kg
54.3
Withings

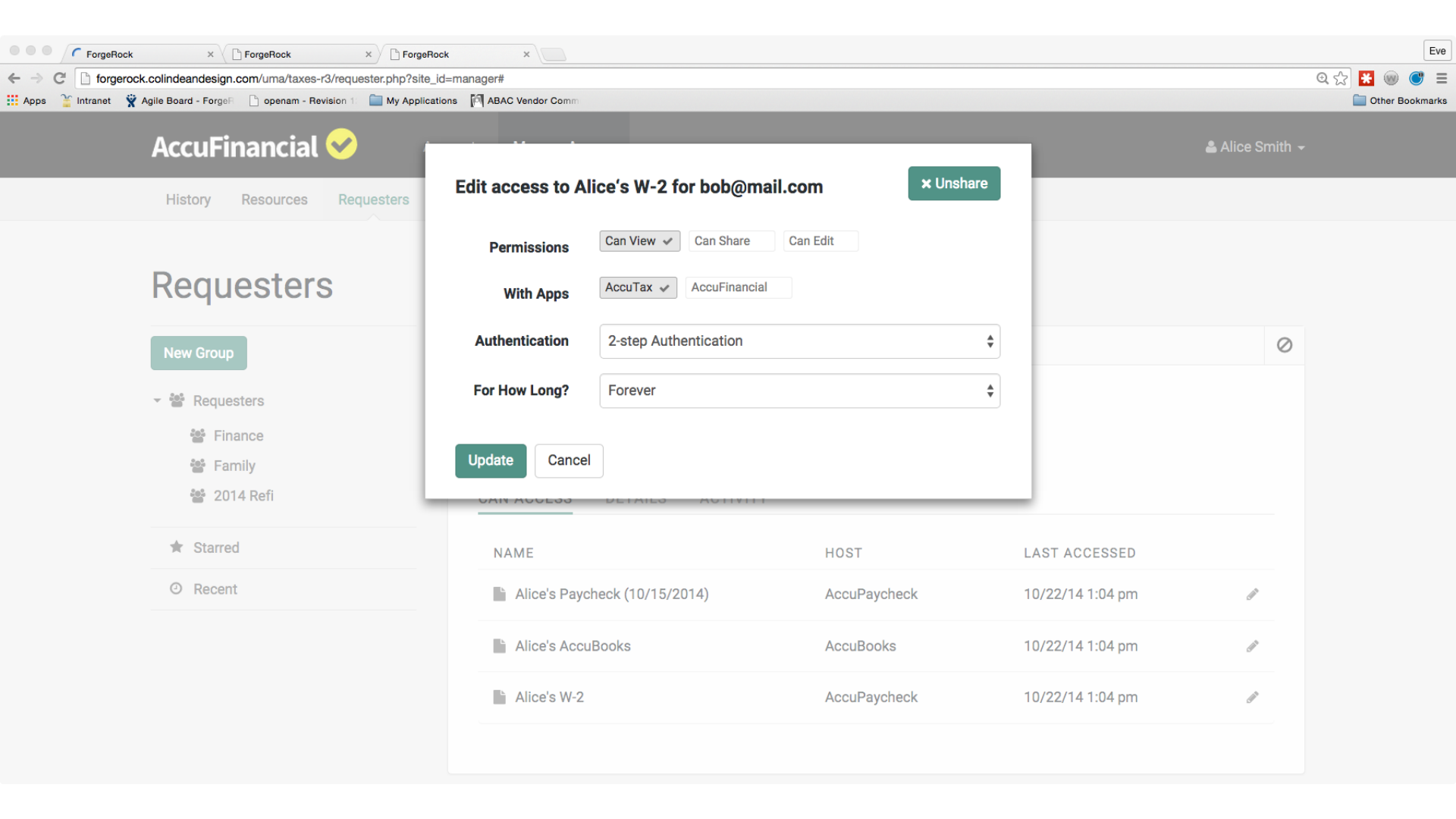
Consent needs to reflect human relationships



Minimum Viable Consent Receipt (MVCR)




ForgeRock
ForgeRock
ForgeRock
forgerock.colindeandesign.com/uma/taxes-r3/requester.php?site_id=manager#
Apps
Intranet
Agile Board - Forge
openam - Revision
My Applications
ABAC Vendor Comm
Other Bookmarks
History
Resources
Requesters
Apps
Pending Requests
Requesters
New Group
Requesters
Finance
Family
2014 Refi
Starred
Recent
Bob Smith
Finance
Family
CAN ACCESS
DETAILS
ACTIVITY
NAME
HOST
LAST ACCESSED
Alice's Paycheck (10/15/2014)
AccuPaycheck
10/22/14 1:04 pm
Alice's AccuBooks
AccuBooks
10/22/14 1:04 pm
Alice's W-2
AccuPaycheck
10/22/14 1:04 pm

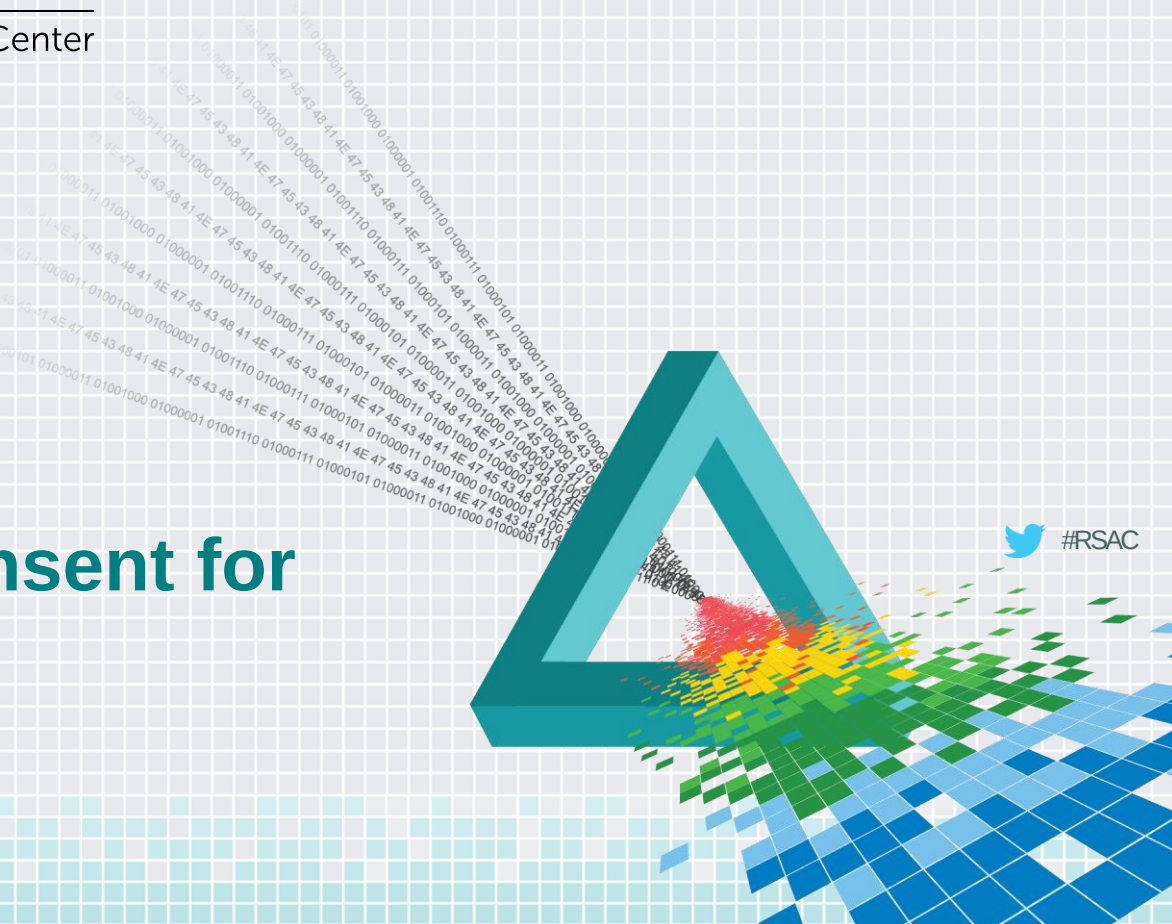

ForgeRock
ForgeRock
ForgeRock
forgerock.colindeandesign.com/uma/taxes-r3/requester.php?site_id=manager#
Apps
Intranet
Agile Board - Forge
openam - Revision
My Applications
ABAC Vendor Comm
Other Bookmarks
AccuFinancial
Alice Smith
History
Resources
Requesters
Requesters
New Group
Requesters
Finance
Family
2014 Refi
Starred
Recent
Edit access to Alice's W-2 for bob@mail.com
Unshare
Permissions
Can View
Can Share
Can Edit
With Apps
AccuTax
AccuFinancial
Authentication
2-step Authentication
For How Long?
Forever
Update
Cancel
NAME
HOST
LAST ACCESSED
Alice's Paycheck (10/15/2014)
AccuPaycheck
10/22/14 1:04 pm
Alice's AccuBooks
AccuBooks
10/22/14 1:04 pm
Alice's W-2
AccuPaycheck
10/22/14 1:04 pm

What does an enterprise share button look like?

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Don’t Confuse Consent for Context



Imagine a chemistry lab

No labels = Grim surprises

Strictest handling procedure must be applied for all jars

But I know what's on that shelf

But what happens when we give a sample to another lab?

This is how enterprises operate

Using Metadata for Good!

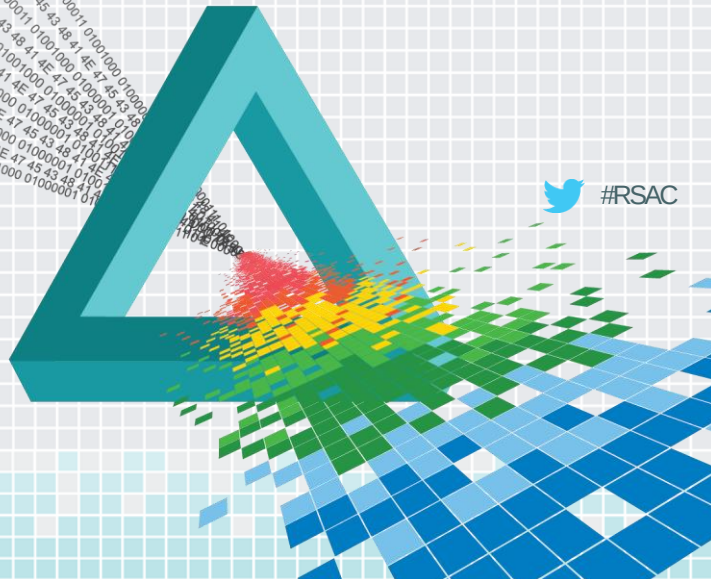
- Durable metadata to describe context
- Relationship Context Metadata (RCM)
  - Optimized for the humans
  - Models relationships
  - Parties and their relationships
  - Consented Uses and Disclosures
  - Obligations
  - What do to if you aren't one of the parties

Metadata is easily separated from data – does RCM suffer from the same flaws?

RSAConference2015

San Francisco | April 20-24 | Moscone Center

IoT Relationships Must Encompass a New World of Transience and Persistence



#RSAC

Information wants to be free

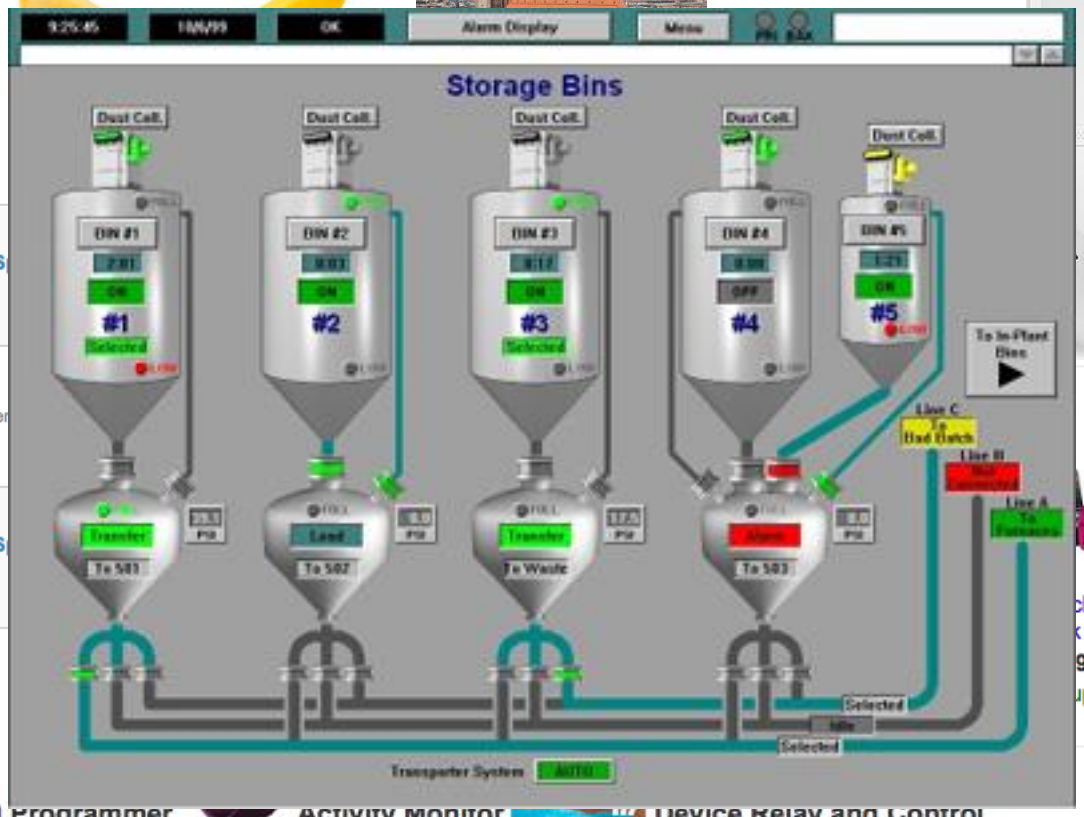
Information wants to live in systems forever

Sort by: Reviews

SONOS PLAY: 5 Wireless S
Audio Speaker

Nest Learning Thermostat
Gateway / Hub: Open Ecosyster
Thermostat

SONOS PLAY: 3 Wireless S
Audio Speaker



Sponsored

chers Go
k Activity...
99
upon.com

Garmin Vivofit
Fitness Activit...
$119.95
Heart Rate M...

ICD

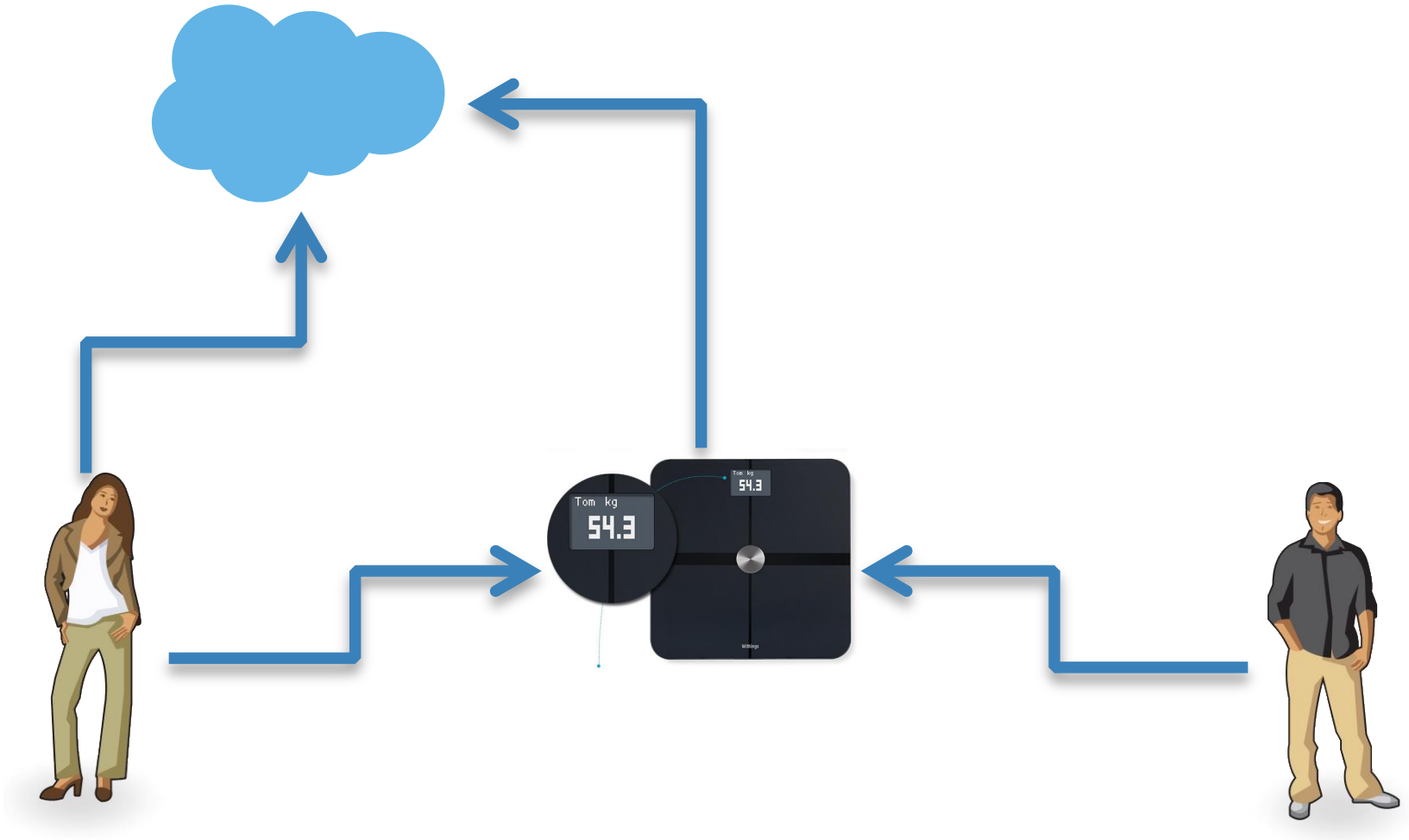
ICD Programmer

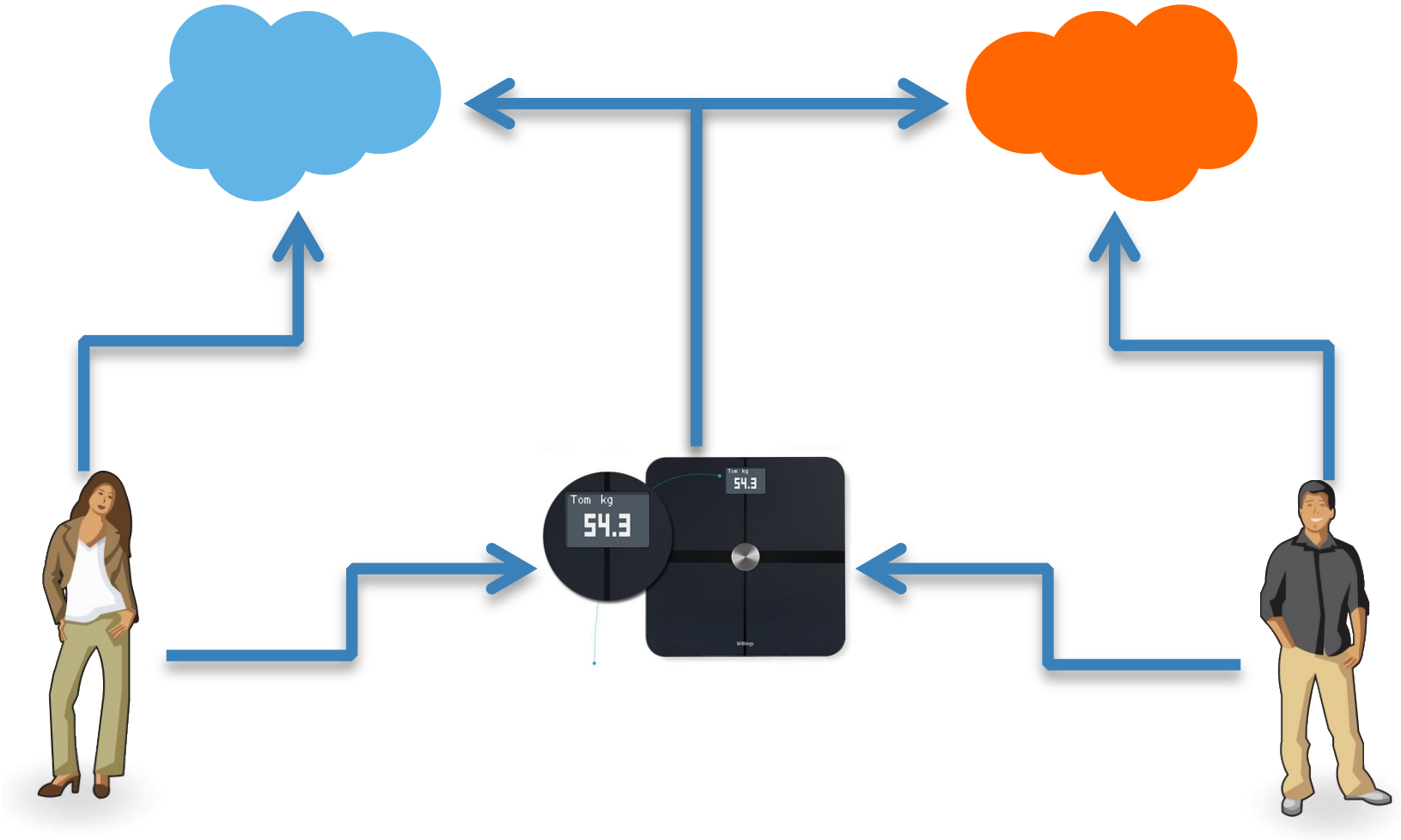
Activity Monitor

Device Relay and Control

Provisioning is like a wedding – or is it?


Tom kg
54.3
Tom kg
54.3


Tom kg
54.3
Tom kg
54.3

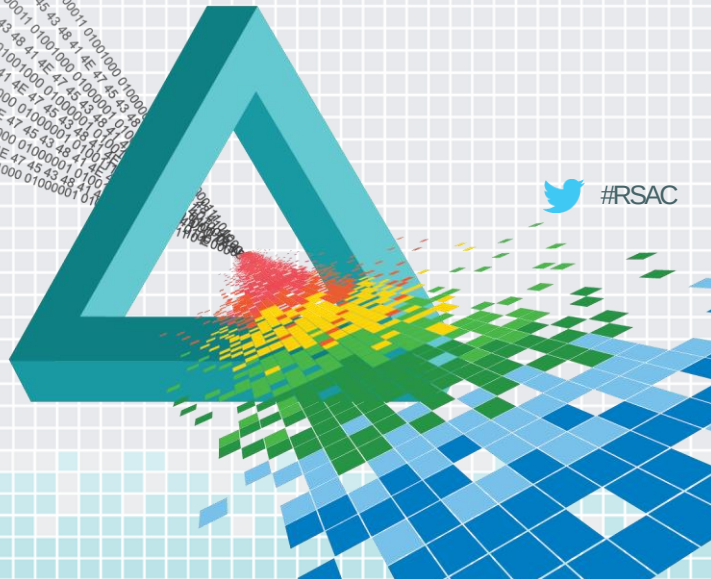

Tom kg
54.3
Tom kg
54.3

So what’s new here? Does there need to be something new here?

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Wrap-Up



Doing sums

- My IRM just killed your IAM
- My relationships just killed your consent
- Context isn’t consent
- Provisioning has to catch up to modern relationships

Classic IAM

Classic IAM

=

Classic IAM

=

OK

Connected World

Connected World

=

Connected World

=

Hilariously Outgunned

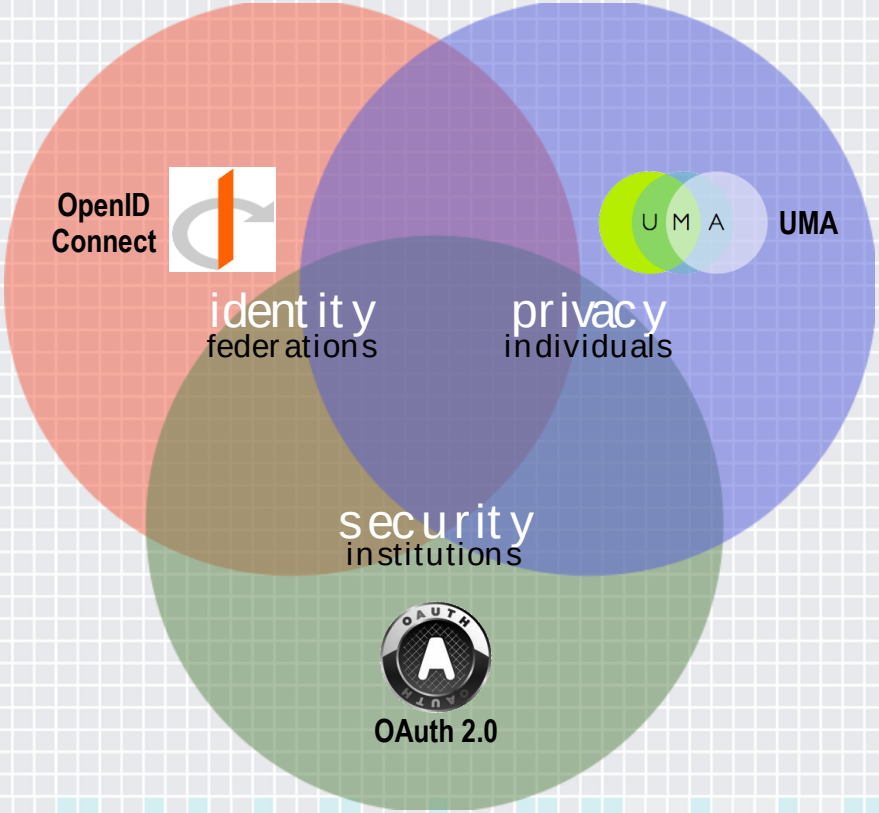
Apply: What to do next week

- Take an inventory of the number of “things” you interact with in the course of a day
- Count the number of people you email (or don’t that might be depressing)
- This will give you a local sense for the scope of the problem
  - Specifically you’ll have a feel for the high scale needs you might have

Apply: What to do after that

- Is OAuth useful for the enterprise?
- If you said no, then…
  - Run through an OAuth tutorial
    - Regardless of whether you believe us on this Relationship stuff, you'll need to understand OAuth at least for mobile and API integrations
- If you said yes, then…
  - Inspect your IAM services and architecture with OAuth, REST, and Relationships in mind
  - Look for low scale services that really need to be high scale

The New Venn of Access Control



Resources

- Kantara Identity Relationship Management WG (@IRMWG)
- Kantara User Managed Access WG (@UMAWG)
- Kantara Identity of Things WG
- Kantara Consent & Information Sharing WG
- OAuth
- OpenID Connect