RSA Conference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: IDY-R04F

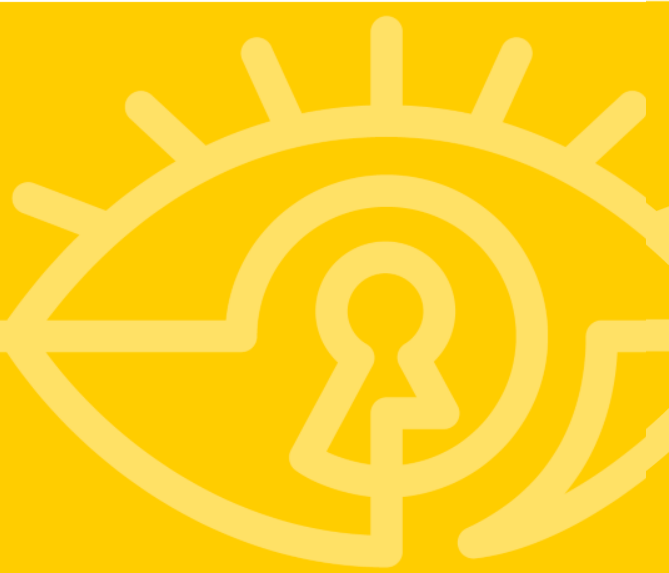
Umpires, Selfie Sticks, and Privacy – Things That Exist But Shouldn't

Joshua Alexander
Director, Product Management
Salesforce
@toopherjosh

Eve Maler
VP Innovation & Emerging Technology
ForgeRock
@xmlgrrl

Gameplan

- The role of tech in privacy *(or, what's with the umpires and selfie sticks?)*
- Issues of privacy in analog vs. digital life
- Tensions in sharing data selectively
- Privacy and/or business
- How much of privacy is about consent?
- Consent tech yesterday, today, and tomorrow
- What to do about all this

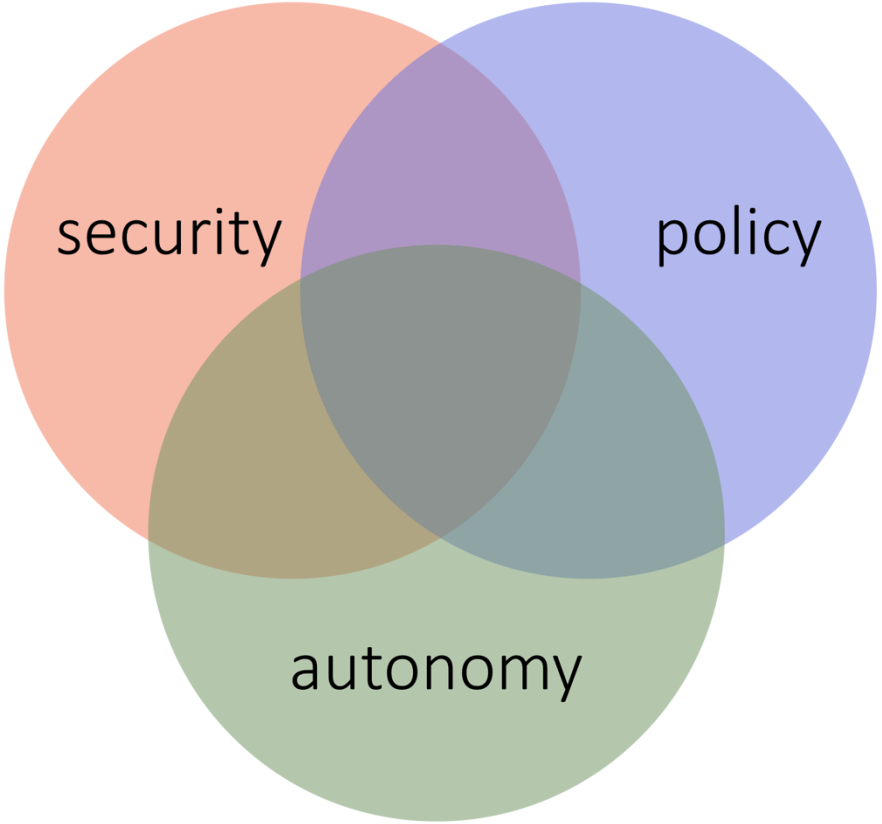


The role of tech in privacy

There's having the tech, and then there's using the tech

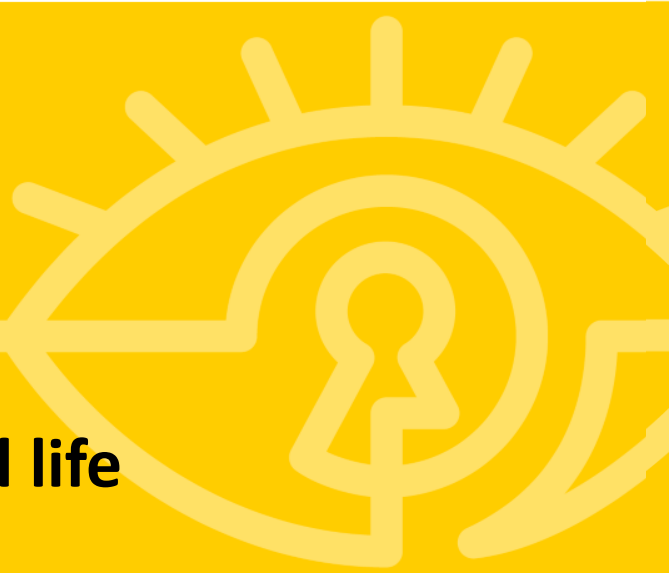
USE IT? \ HAVE IT?	YES	NO	MIXED
DON'T			
DO BUT SHOULDN'T			
IT'S COMPLICATED			

Why is it complicated?
Look at its many guises



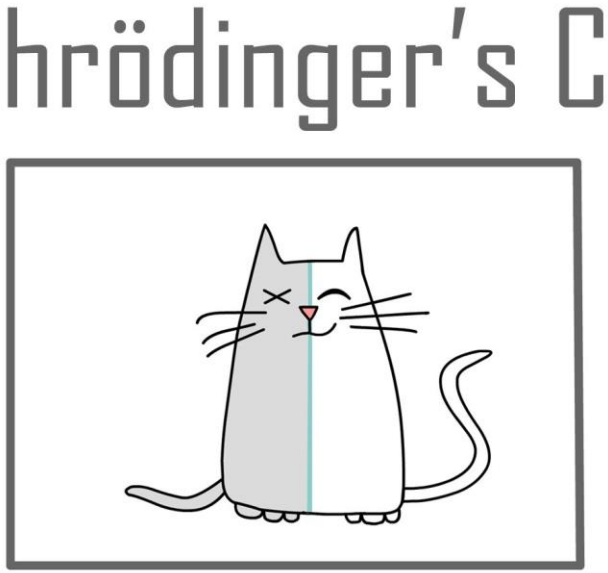
Preserve individuality – at what cost?

Jumping the individual gap



Issues of privacy in analog vs. digital life

If you didn't measure it, did the data exist?



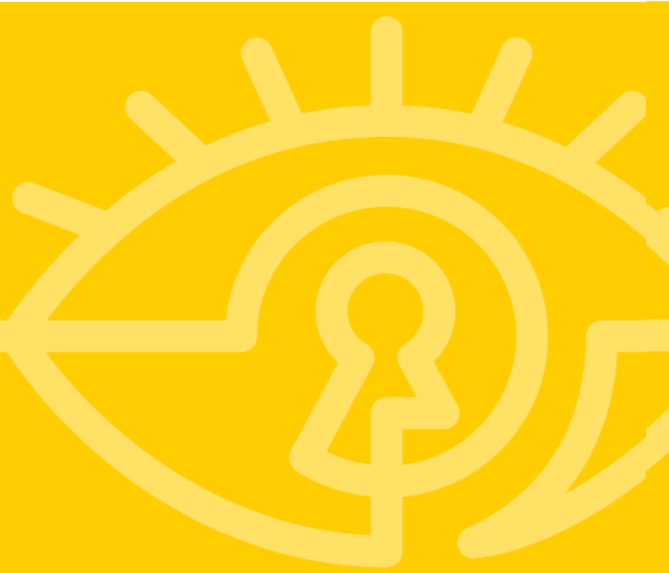
Data ownership vs. data control

Patient records

- Why does it takes *weeks*?

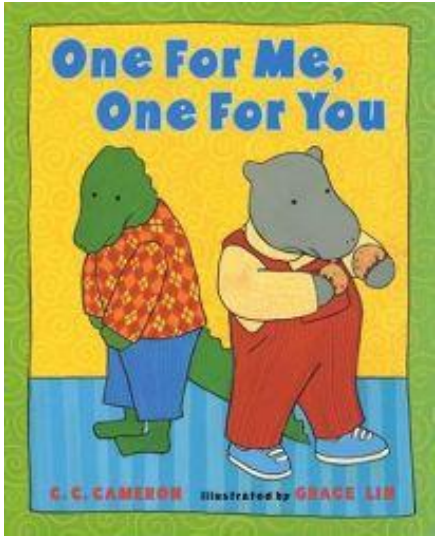
Do we measure the right things?

- Do we incentivize the measurement of the right things?

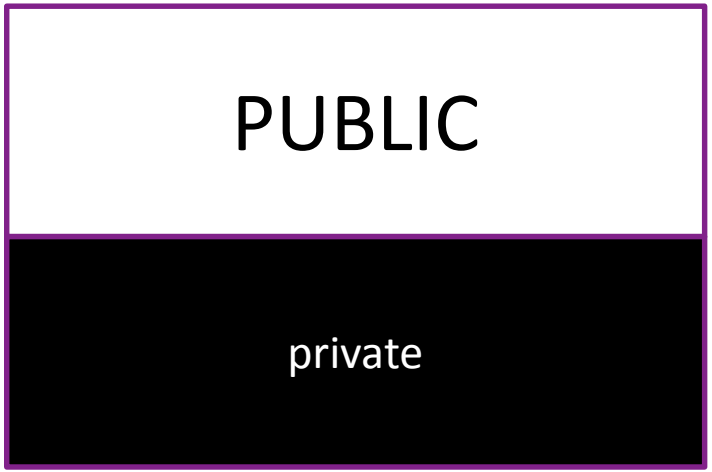


Tensions in sharing data selectively

Our conversations have gotten extremely attenuated



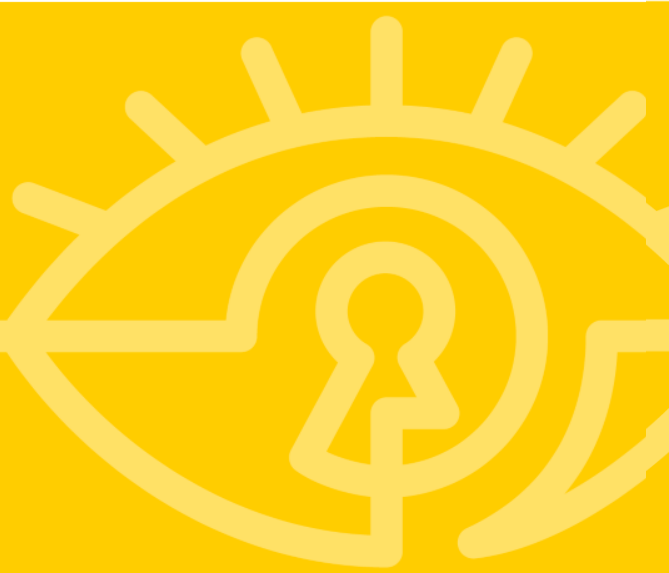
Twitter vs. Facebook



- Public
  - Friends
    - Friends of friends
      - Friends of friends of friends
        - Friends of friends of friends of friends…

Online sharing between people comes with a MITM-by-design

Bob Eve Alice



Privacy and/or business

Human beings vs. privacy practitioners

unconcerneds

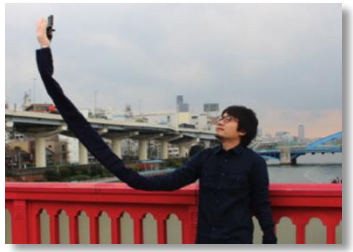
fundamentalists

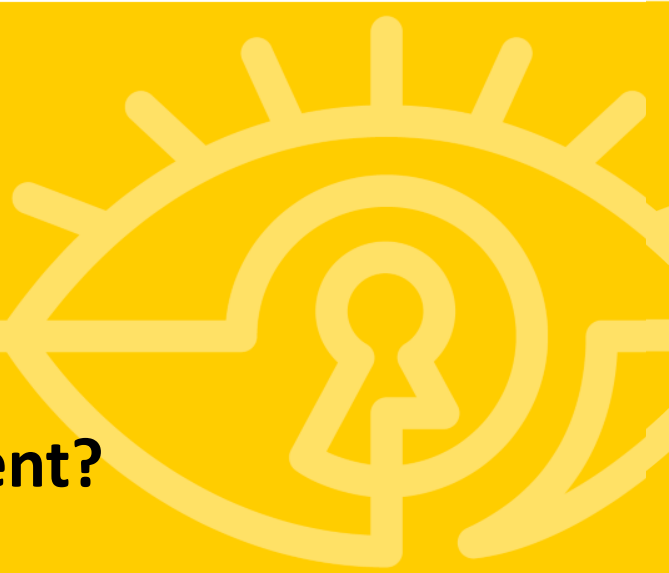
pragmatics

practitioners

There are only so many business models

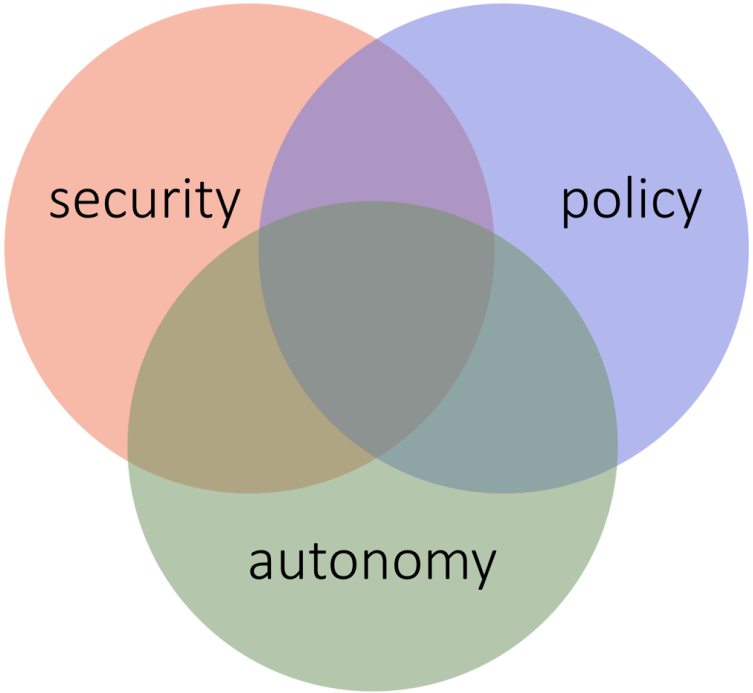
- How do people pay for service? Some combination of…
  - Money
  - Time/attention
  - Data
- What people express concern about and what they are willing to pay money for are two different things
- But all types of people can *lose trust* easily





How much of privacy is about consent?

Depending on how you count…

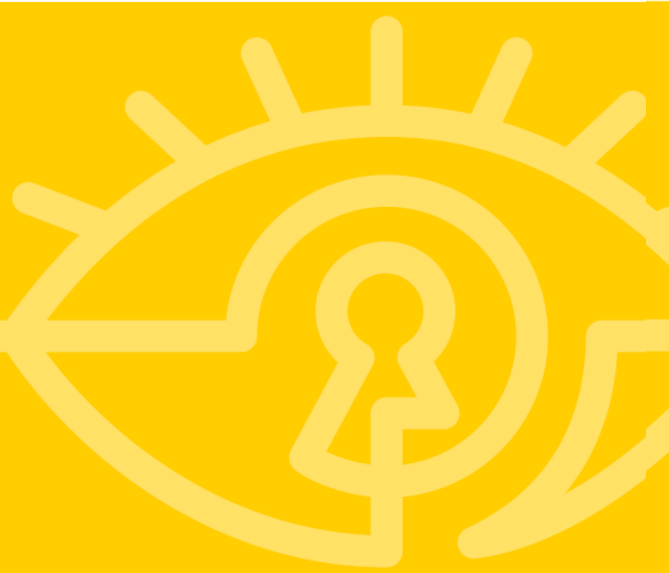


Ten key developments in the EU GDPR:

- Data Protection Officers
- **Explicit consent** and lawfulness of processing
- **Data portability and access rights**
- **Right to be forgotten**
- Data protection by design and default
- Data transfers and the ‘anti-FISA clause’
- Freedom of expression and journalism
- Measures based on profiling
- Breach notifications
- Data Protection Impact Assessments

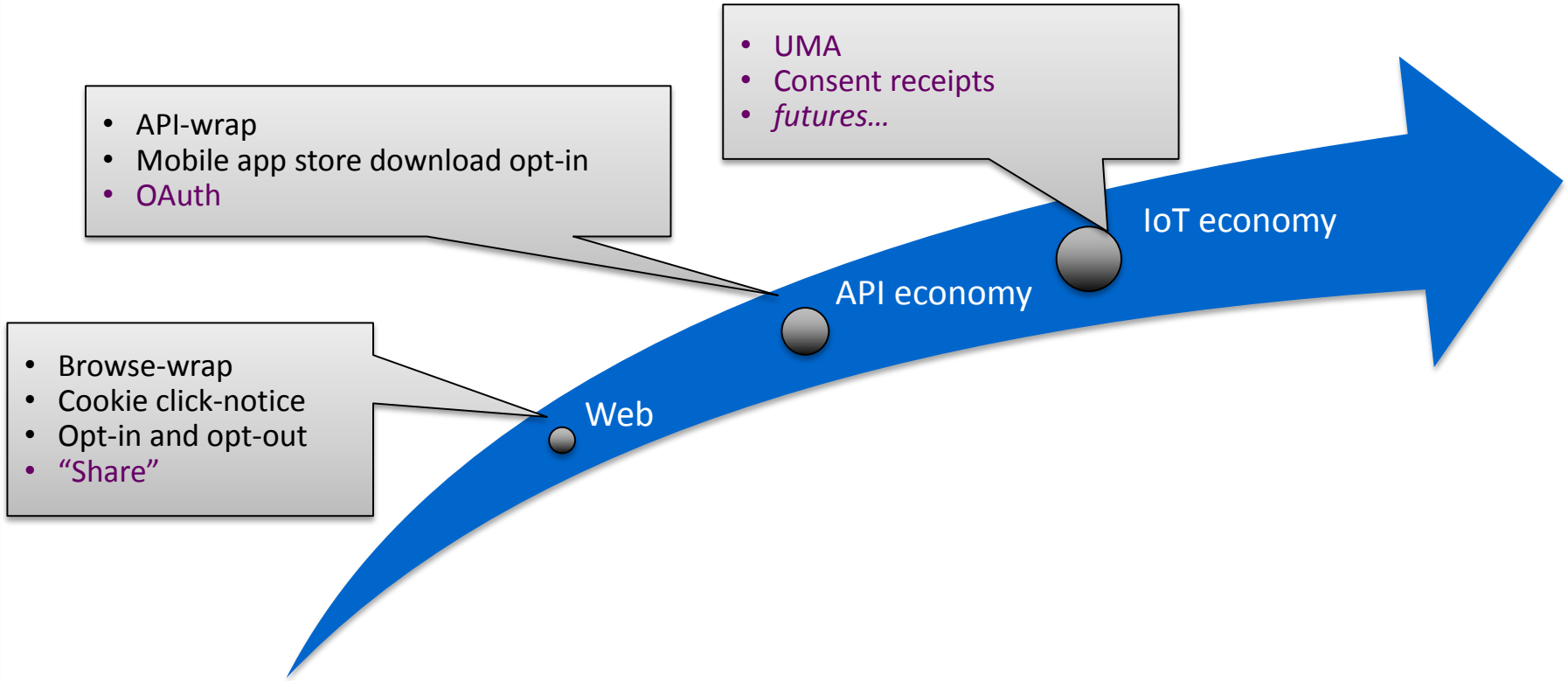
Consent has a role in a new theory of strategic risk mitigation

explicit consent to agreements based on model clauses



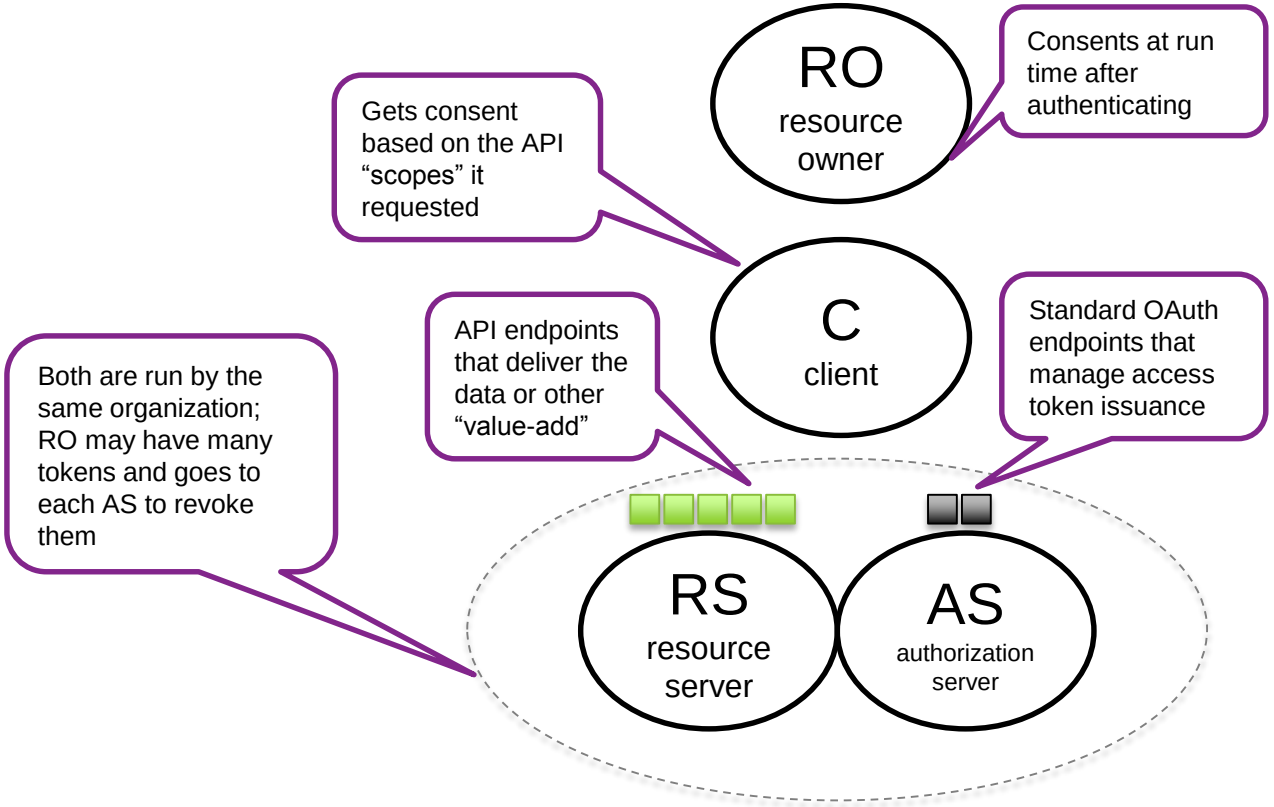
Consent tech yesterday, today, and tomorrow

Things are actually improving



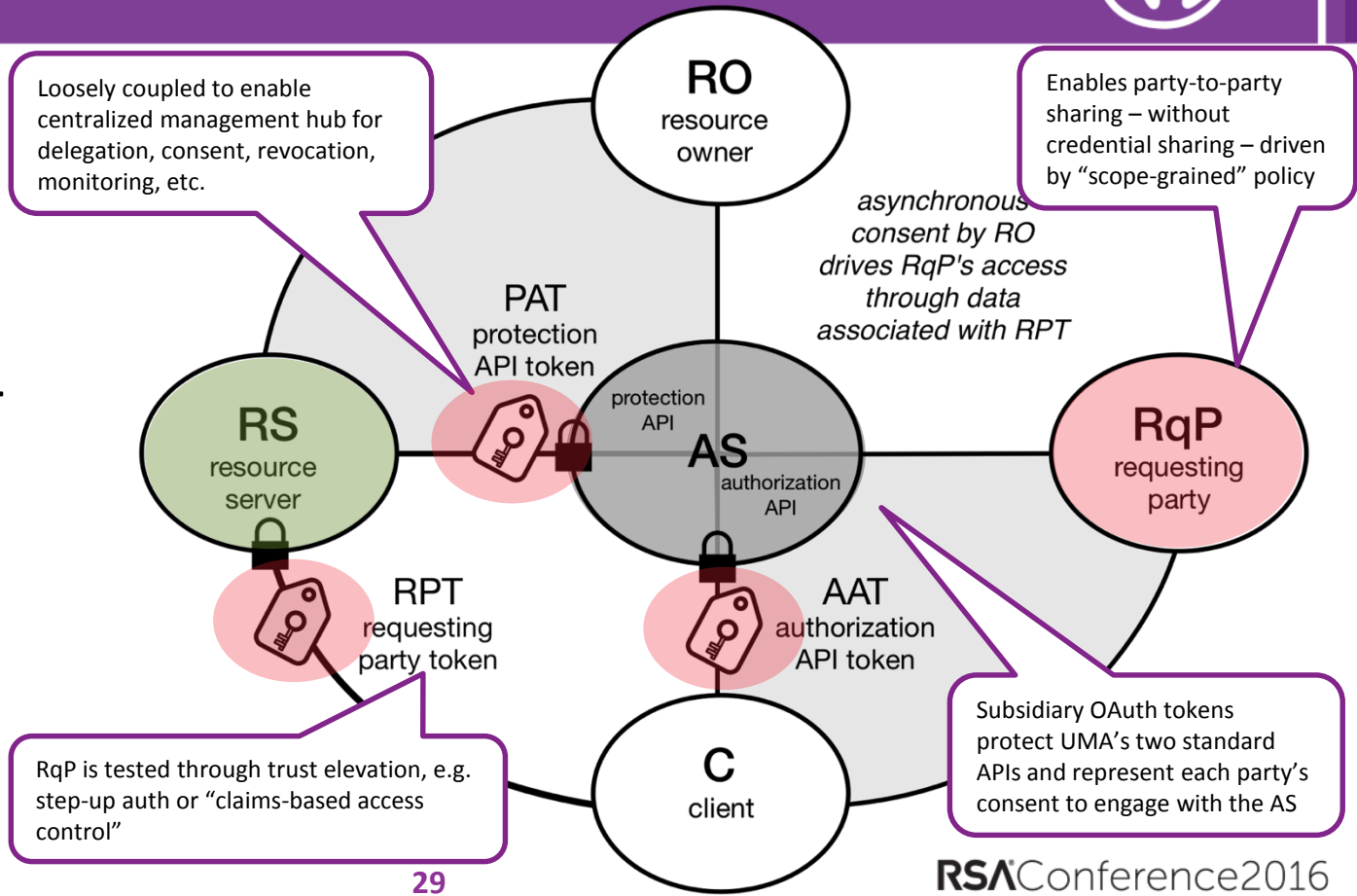
How does OAuth work?

OAuth is about consented app connections on behalf of one party (think “social login”)

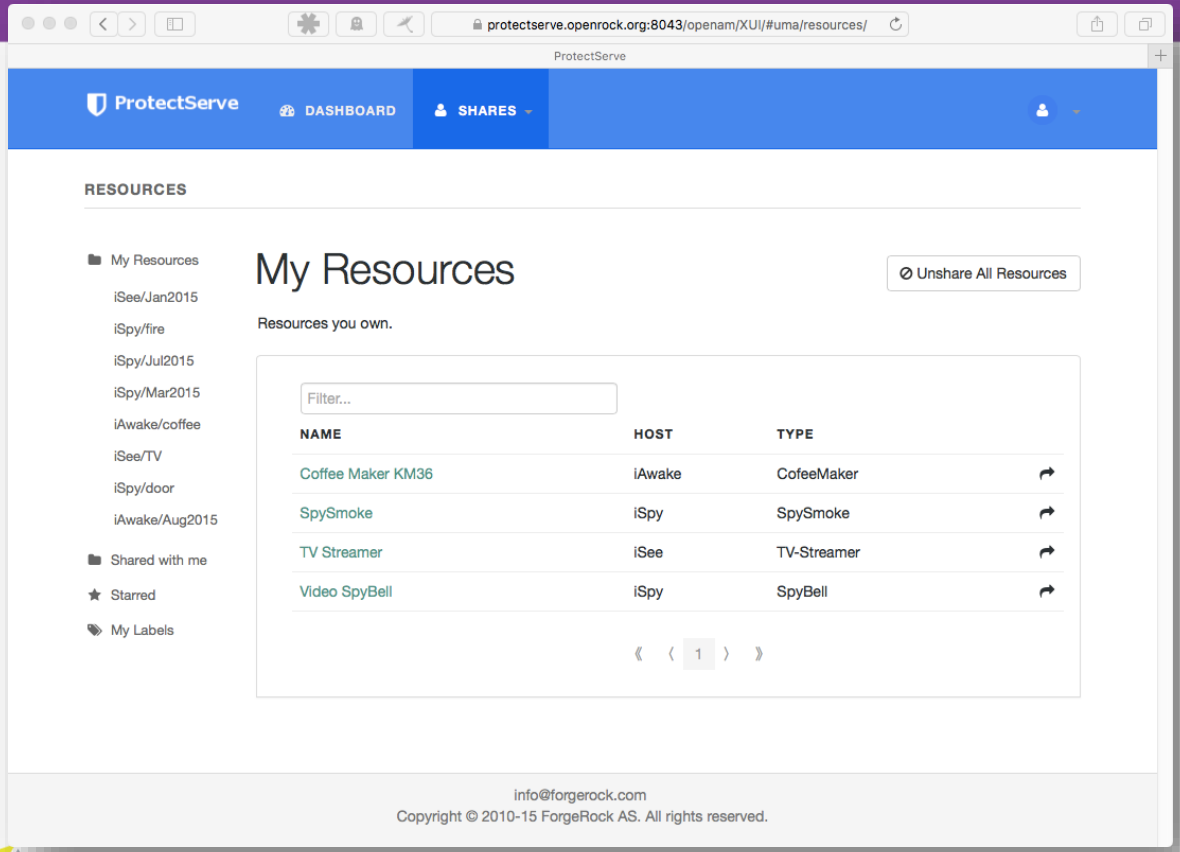


How does UMA work?

UMA leverages OAuth to enable party-to-party consent and delegation



A sample UX


protectserve.openrock.org:8043/openam/XUI/#uma/resources/
ProtectServe
ProtectServe
DASHBOARD
SHARES
RESOURCES
My Resources
iSee/Jan2015
iSpy/fire
iSpy/Jul2015
iSpy/Mar2015
iAwake/coffee
iSee/TV
iSpy/door
iAwake/Aug2015
Shared with me
Starred
My Labels
My Resources
Unshare All Resources
Resources you own.
Filter...
NAME
HOST
TYPE
Coffee Maker KM36
iAwake
CofeeMaker
SpySmoke
iSpy
SpySmoke
TV Streamer
iSee
TV-Streamer
Video SpyBell
iSpy
SpyBell
1
info@forgerock.com
Copyright © 2010-15 ForgeRock AS. All rights reserved.

Consent receipts

Receipt Contents

Jurisdiction

US

Timestamp

Mon Jan 25 2016 19:59:55 GMT-0800 (PST)

Method Of Collection

web form

Consent Processor

http://www.consentreceipt.org/

Unique ID

fbba510d25043e10711687286367aebf91ffacbd74b576616dc06b28e09a56787cc84dcfe95762bea4b80b127495767d09a260c37b8df243d2f41a3a86a80ada

PII Principal

example@example.com

Data Controller

is acting on behalf of company: yes
Contact Name: Dave Controller
Company Name: Data Controller Inc.
Address: 123 St., Place
Contact Email: dave@datacontroller.com
Phone Number: 00-123-341-2351

Privacy Policy URL

http://example.com/privacy

Purposes

None

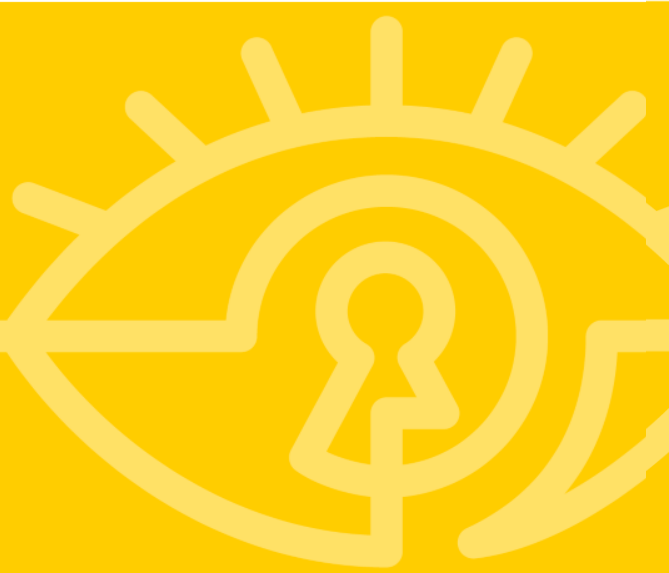
Sensitive Personal Information

None

3rd party sharing of personal information

Sharing None data to 3rd Party Name or/3rd Party Category for the purpose of None purpose

Futures



What to do about all this:
Apply what you've learned today

If you're a privacy practitioner

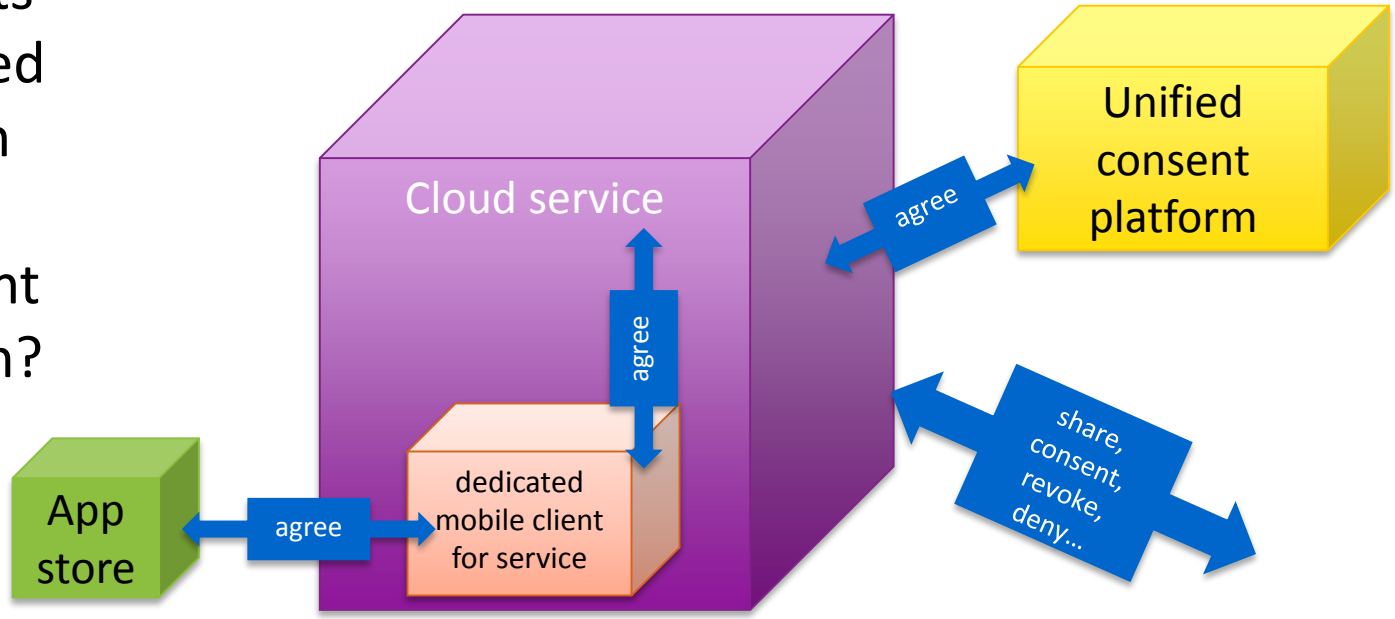
- Next week:
  - Reach out to business owner counterparts to ask about "consent vulnerabilities" beyond compliance risk
- In three months:
  - Begin investigating personal data as a *mutual* corporate and customer asset

If you're a privacy practitioner (cont'd)

- In six months:
  - Collaboratively draw up plans to build more trusted digital relationships that address the autonomy element of privacy for well-rounded business benefit
    - Privacy and data protection policy
    - Big data governance
    - Consent strategy

Thinking about consent strategy

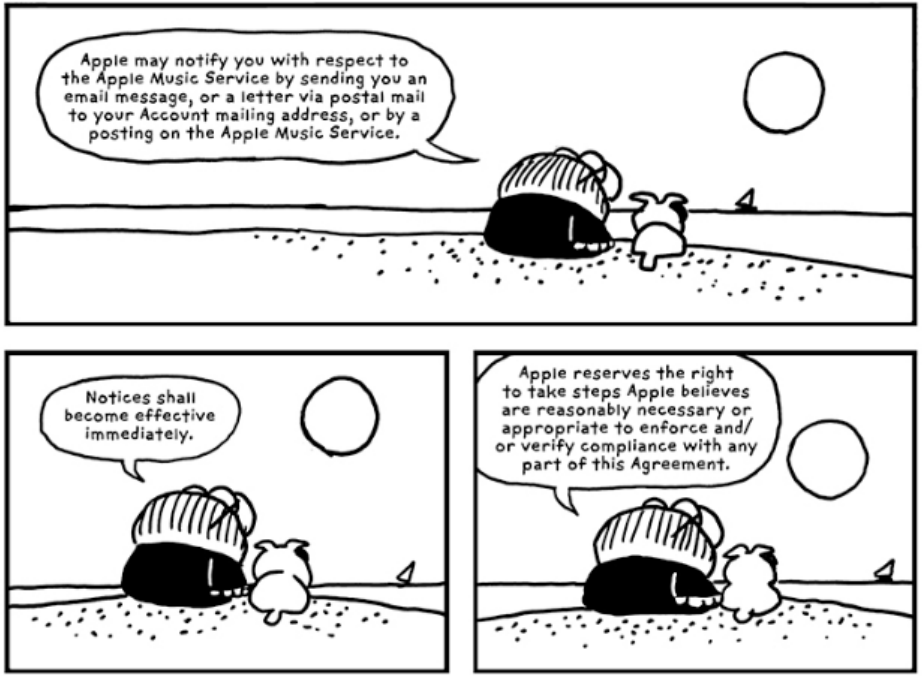
What elements can be deferred until users can monitor and control consent at a finer grain?



If you're a human being

- Next week: Start asking key questions about the personal data in your (and your family's) life:
  - Do I actually control this data?
  - If so, how can I access it? How can I control its further distribution?
  - If not, why not? Do I care?

This may require reading some Ts and Cs…



If you're a human being (cont'd)

- In three months:
  - Do a gut check about which services, apps, and personal data situations, if any, left you distrustful or creeped out
  - Decide what your reasonable next actions are
    - Lifestyle change
    - Communications/community
    - …
- In six months:
  - Assess the effectiveness of your actions
  - Assess the changes in data volumes and sources in your life

Examples

- Music services
- Sleep apps
- Fitness watches
- Employee health programs
- Retail loyalty programs

This afternoon

- Come to our Focus-On Q&A (W2014)!