RSAConference2017
San Francisco | February 13 – 17 | Moscone Center

POWER OF OPPORTUNITY

SESSION ID: IDY-R03

Designing a New Consent Strategy for Digital Transformation

Eve Maler
VP Innovation & Emerging Technology
ForgeRock
@xmlgrrl

Digital transformation challenges

End-users: increasingly mistrustful but still demanding in other ways

DEC 14, 2016 @ 10:06 AM 24,508 VIEWS

Evernote's New Privacy Policy Allows Its Employees To Access Your 'Ideas'

Thomas Fox-Brewster,
FORBES STAFF

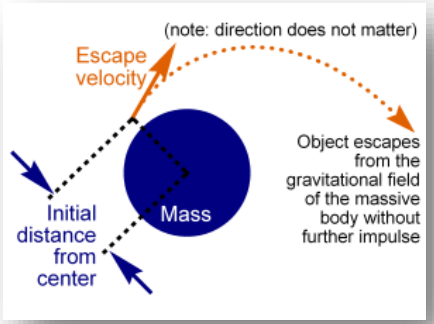
BUT

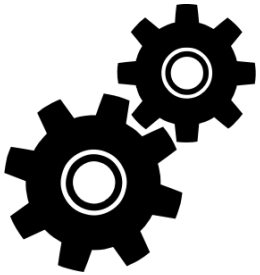
NEWS

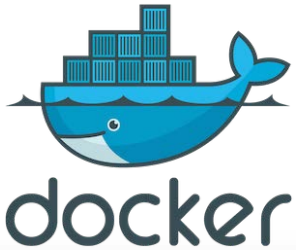
Evernote Revisits Privacy Policy Change in Response to Feedback

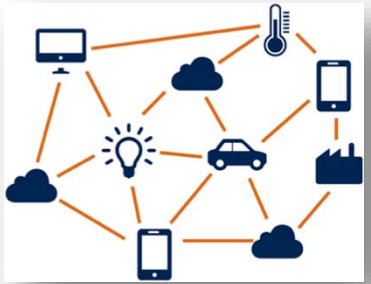
Posted by Greg Chiemingo on 15 Dec 2016

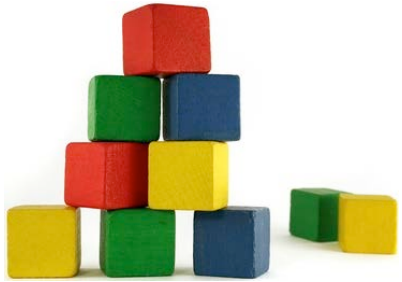
The innovation and industry context: never more…interesting





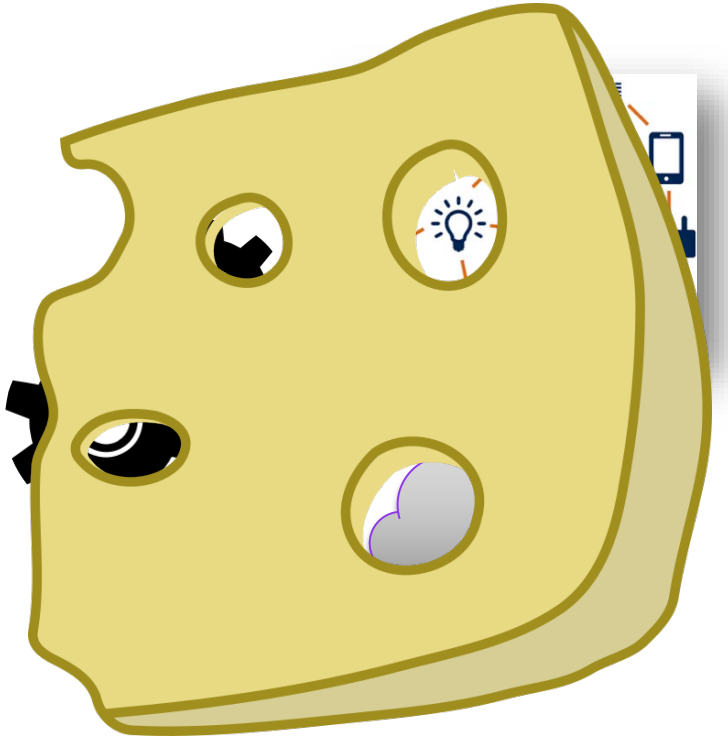






FORGEROCK

The risk context: forever playing not to lose



KEEP CALM AND PREPARE FOR THE GDPR

PSD2

HIPAA

The business and risk teams *must* meet in the middle

Risk perspective

"Consent should not be regarded as freely given if the data subject has no **genuine or free choice** or is unable to **refuse or withdraw consent without detriment**. …

In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a **clear imbalance** between the data subject and the controller…"

Business perspective

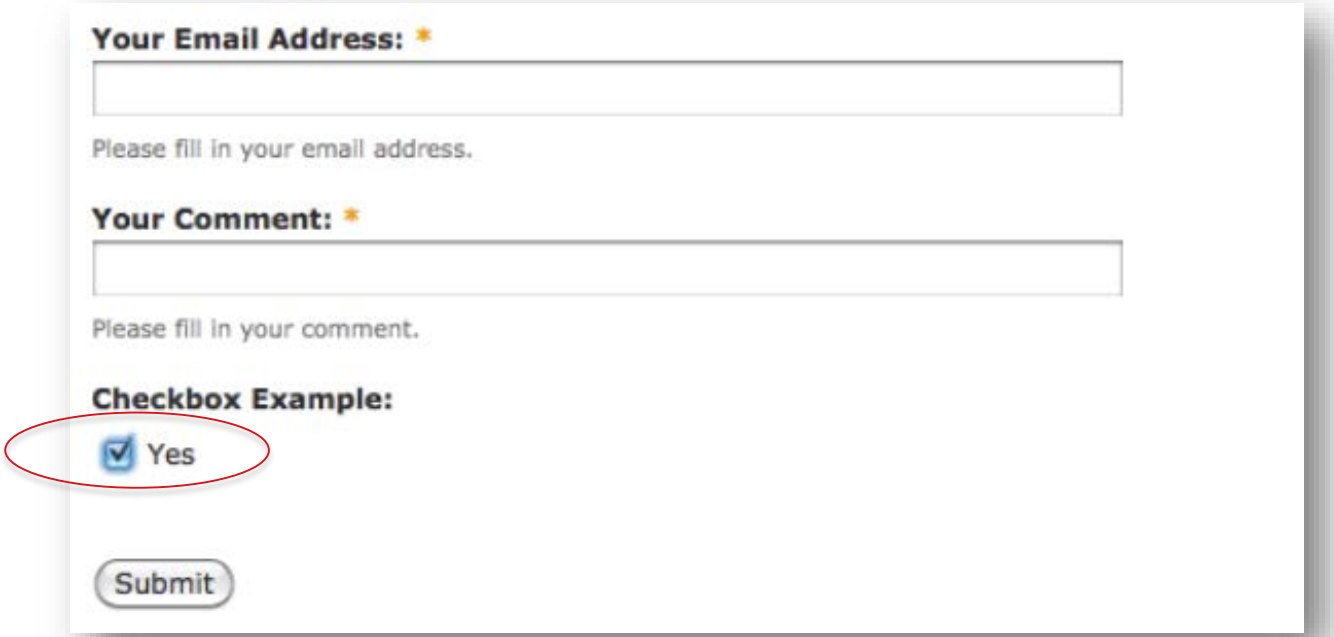
We value personal data as an asset

Our **customers'** wishes have value

Our customers have their **own reasons** to share, not share, and mash up data, which we can address as value-add

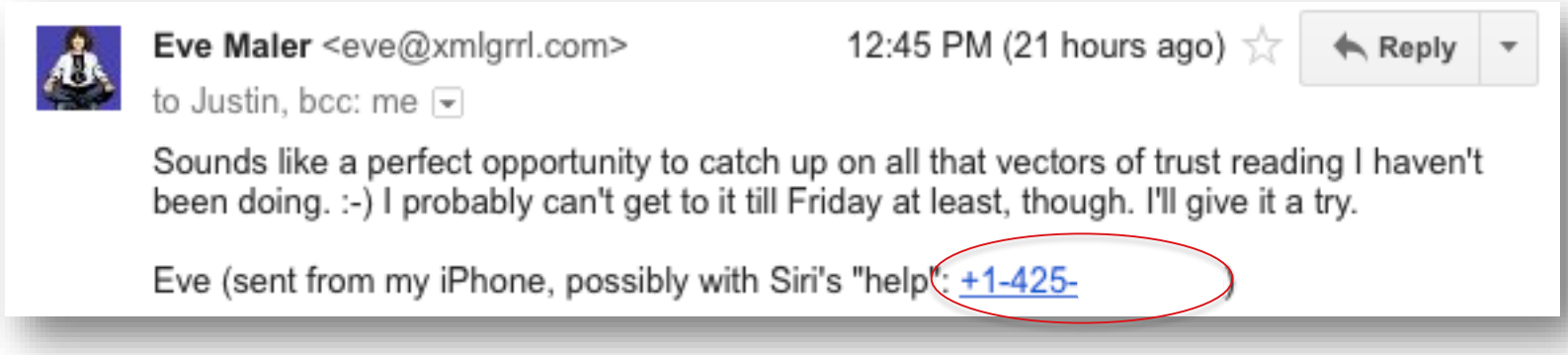
The traditional system of user consent

Opt-in consent



Opt-out consent

Implied consent



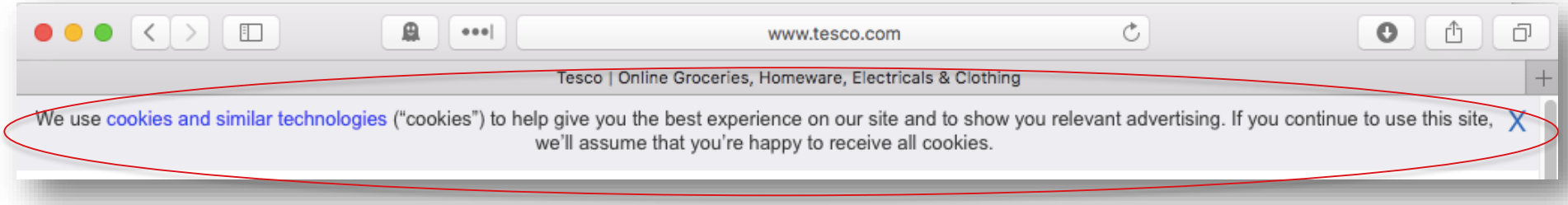
Eve Maler <eve@xmlgrrl.com> 12:45 PM (21 hours ago) ☆ Reply

to Justin, bcc: me

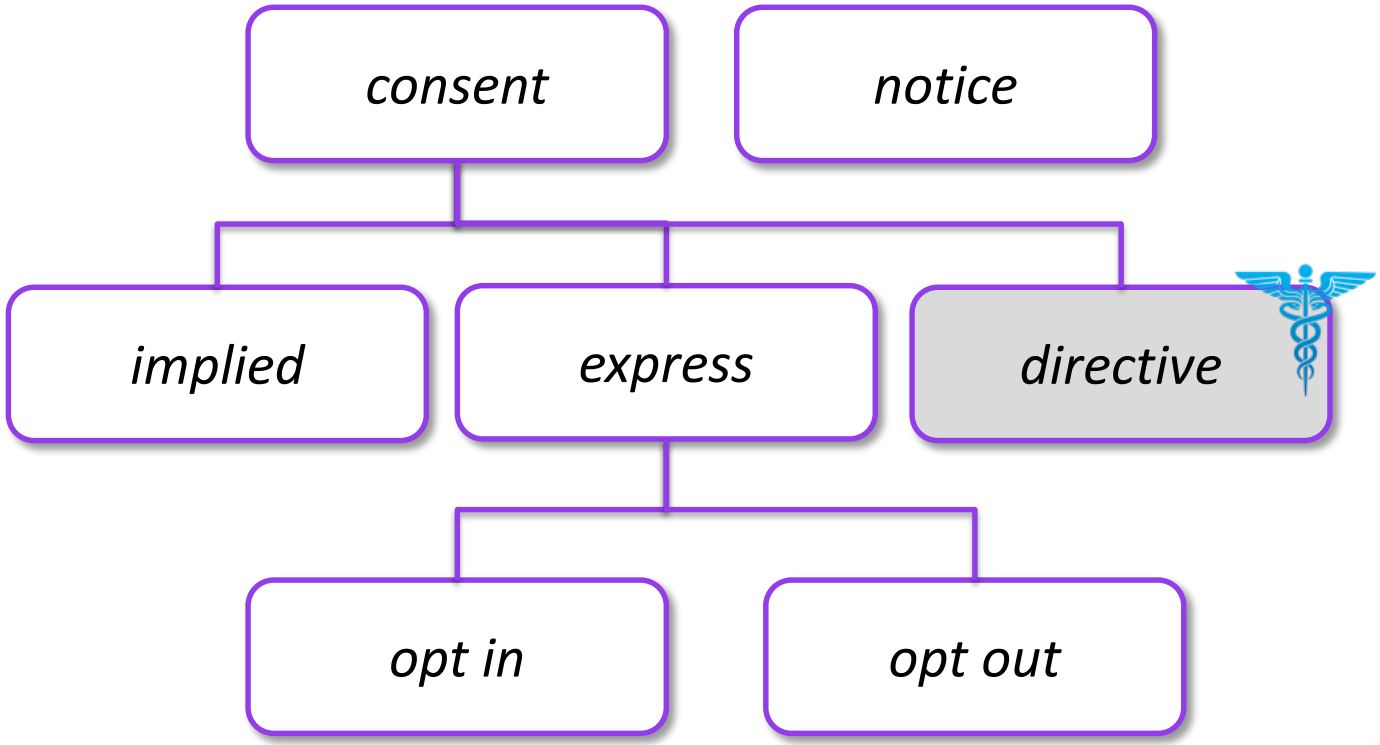
Sounds like a perfect opportunity to catch up on all that vectors of trust reading I haven't been doing. :-) I probably can't get to it till Friday at least, though. I'll give it a try.

Eve (sent from my iPhone, possibly with Siri's "help": +1-425-

Cookie directive

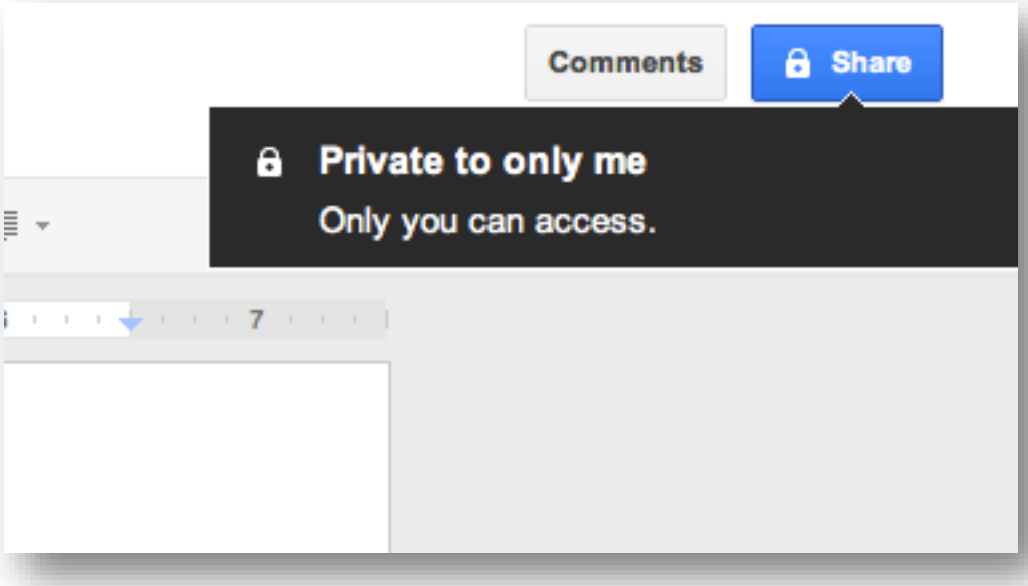


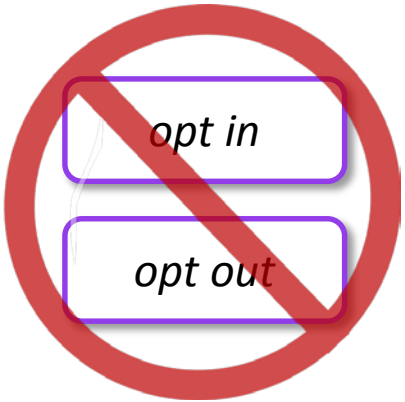
Pretty much the entire *official* world of consent



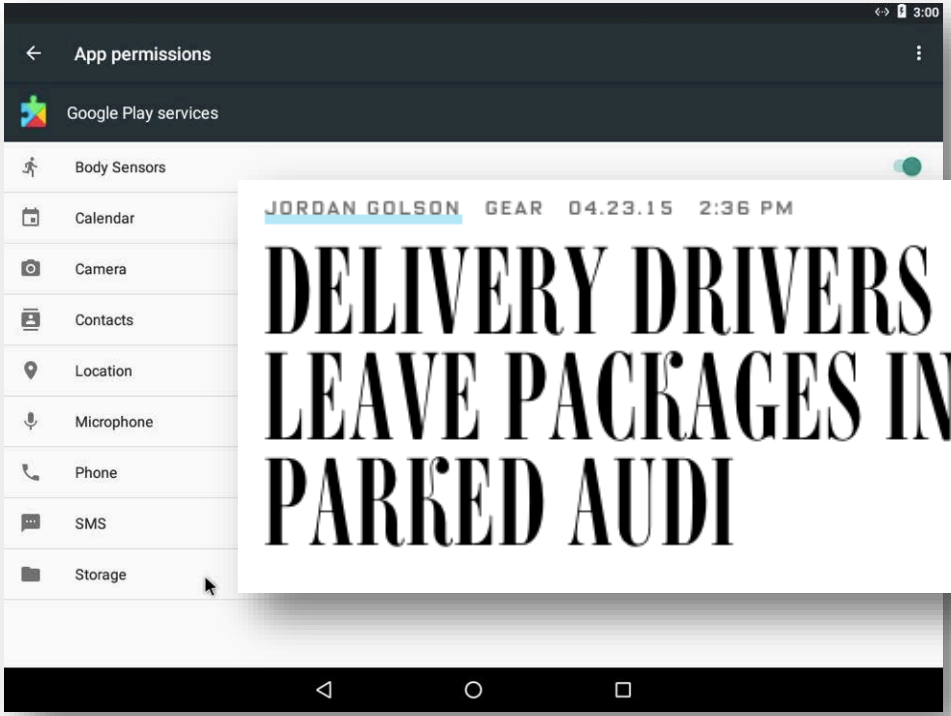
- Collection
- Use (for Purpose)
- Disclosure

What about Google Docs “Share”?





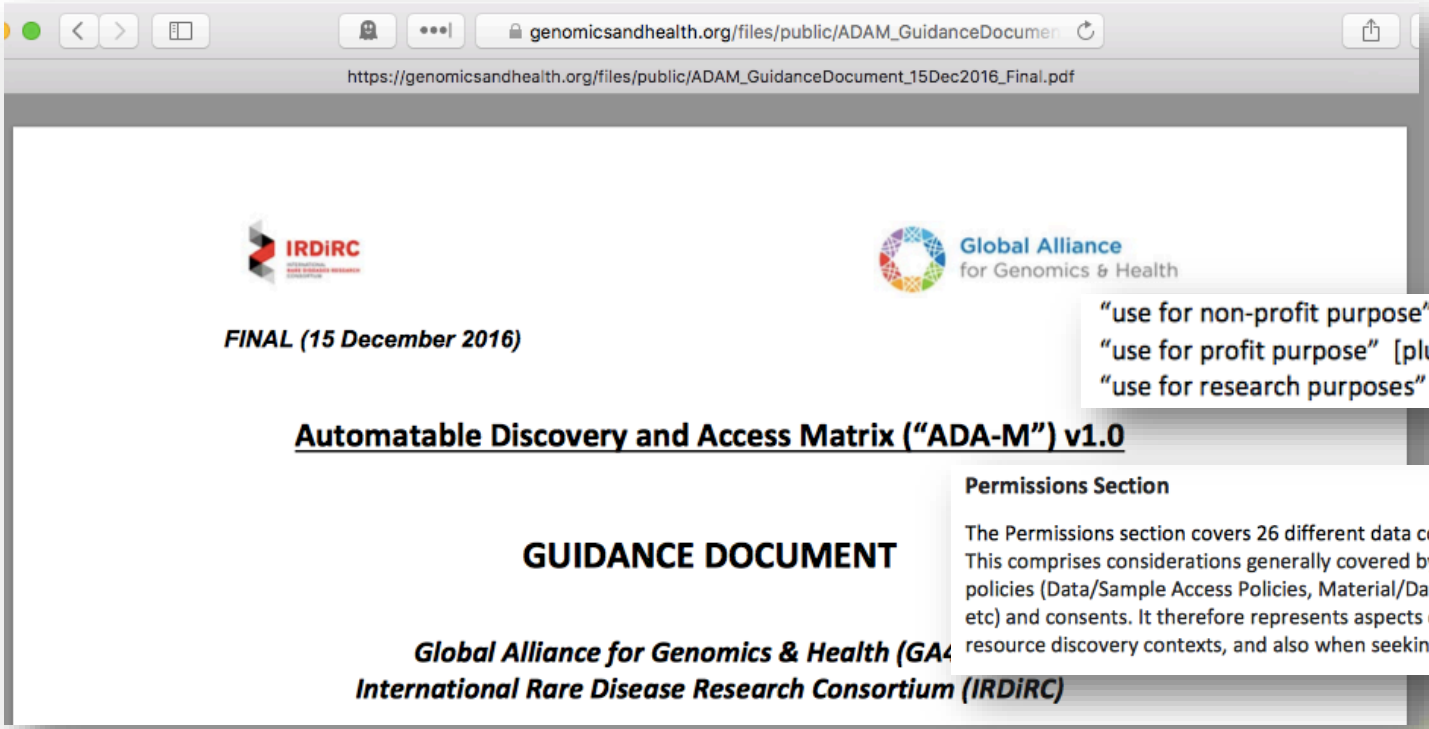
What about Android upgrades? Or unattended package deliveries?



JORDAN GOLSON GEAR 04.23.15 2:36 PM

DELIVERY DRIVERS CAN NOW LEAVE PACKAGES IN YOUR PARKED AUDI

What about GA4GH's ADA-M machine-readable conditions for use of genomic data?



Purpose

"use for non-profit purpose" [plus an associated free text field]
"use for profit purpose" [plus an associated free text field]
"use for research purposes" [plus an associated free text field]

Permissions Section

The Permissions section covers 26 different data concepts ('items') for types of use of a resource. This comprises considerations generally covered by, or otherwise included in, laws, institutional policies (Data/Sample Access Policies, Material/Data Transfer Agreement, Data Access Agreement, etc) and consents. It therefore represents aspects of control which are useful to know about in resource discovery contexts, and also when seeking to actually access a particular resource.

A deeper classification system

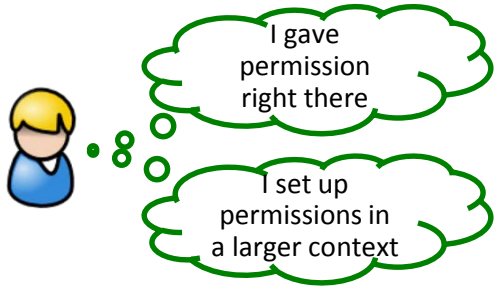
A proposal for a new permission classification system

Modes:

- Directed
- Reactive
- Long-Term

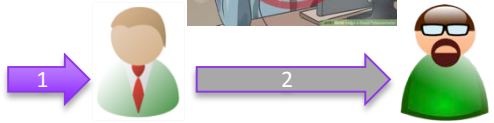
Methods:

- Concrete
- Abstract



Controls:

- Scope
- Grantee
- Environment
- Usage
- Downstream

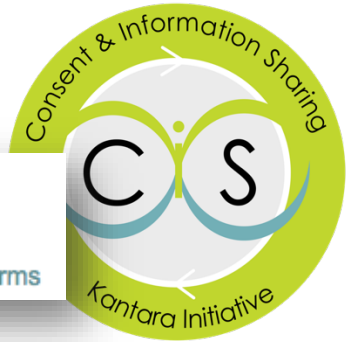


More “consent tech” is arising to meet the digital transformation challenge

Health Relationship Trust (HEART) at OpenID Foundation

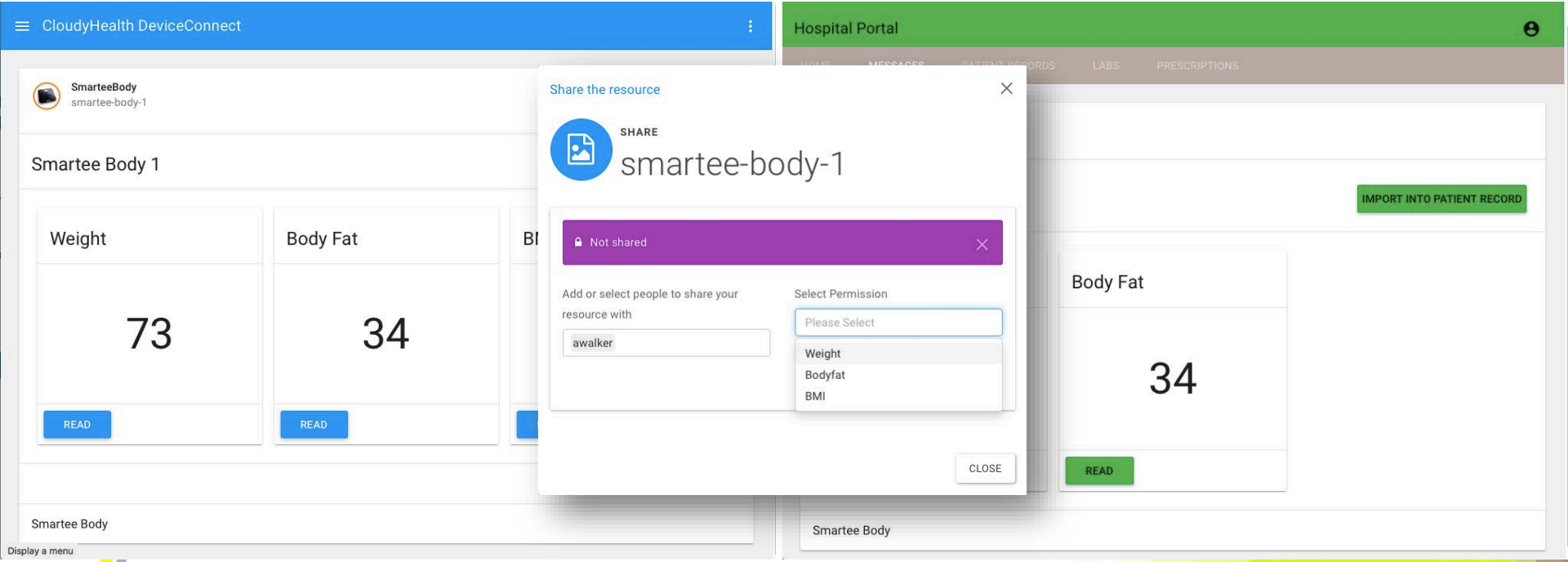
Active Projects:

- Consent Receipts
- User Submitted Terms



Working an example with the User-Managed Access standard (tinyurl.com/umawg)

patient view **proactive sharing flow** **doctor view**



Remember consent directives?

directive

AUTHORIZATION TO DISCLOSE PROTECTED HEALTH INFORMATION
Michigan Department of Health and Human Services

Directions: *Type or Print all requested information, with exception of signatures on Page 2.*

Individual's Name (Beneficiary, Recipient, Patient, Consumer, etc.)			Individual's ID Number (Medicaid, SSN, Other)
Individual's Name			0123456789
Street Address			Individual's Date of Birth
Individual's Address			/ /
City	State	ZIP Code	Phone
			( ) -

I AUTHORIZE THE MICHIGAN DEPARTMENT OF HEALTH AND HUMAN SERVICES (MDHHS) TO SHARE MY HEALTH INFORMATION:

List the amount or type of information you would like to share in the section below.
For example, you can say all my health information or list certain types of information you would like to share.

"All my health information, any time until authorization revoked."

(or any specific information you want to include)

MDHHS MAY SHARE MY HEALTH INFORMATION WITH THE FOLLOWING PERSON OR ORGANIZATION:

Representative and/or Organization Name
Name of Person/Organization

Address of Authorized Representative
Street Address

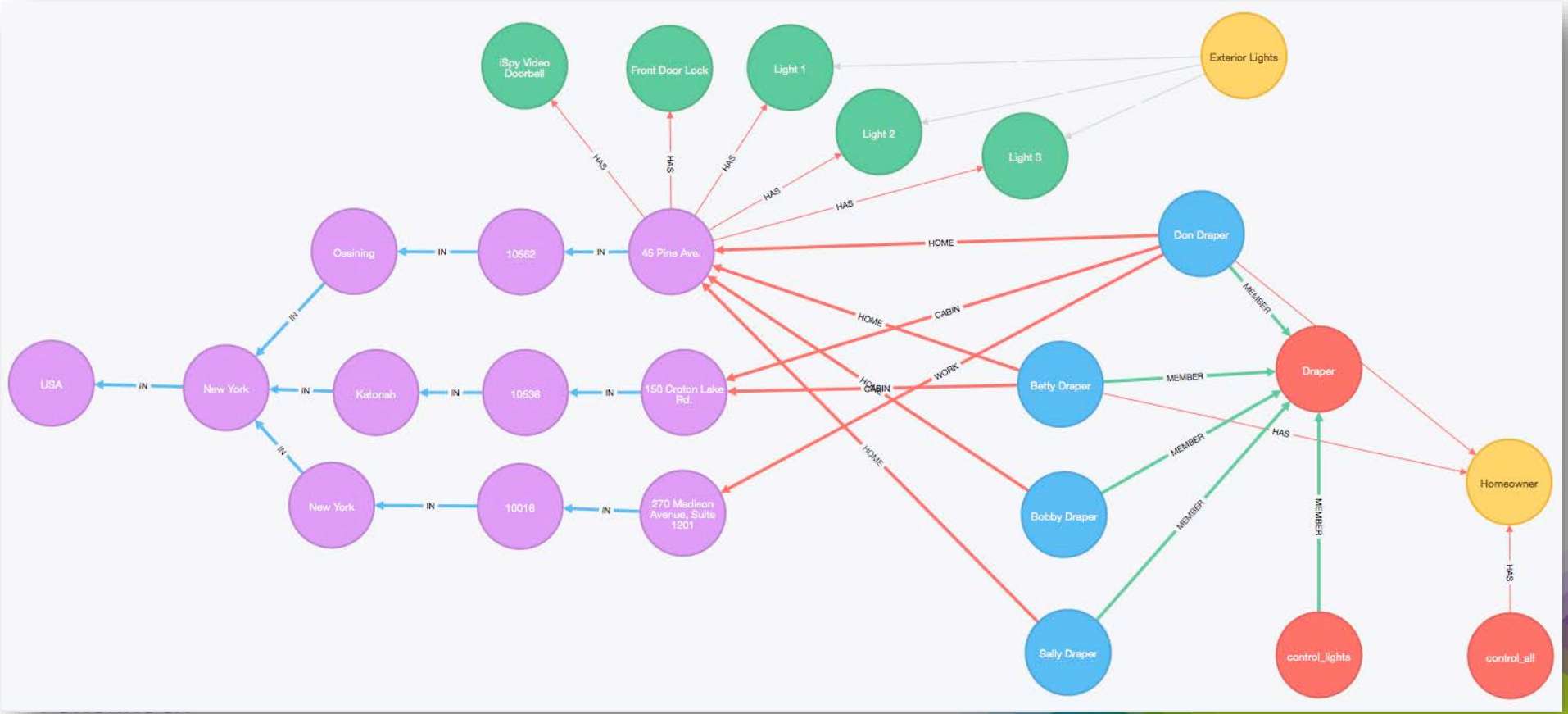
City, State, ZIP Code

( ) - ( ) -
Phone Number Fax Number

SAMPLE

FORGEROCK

Access sharing can even be driven off relationships with people and devices



UMA capabilities (each deployment may differ)

Modes:

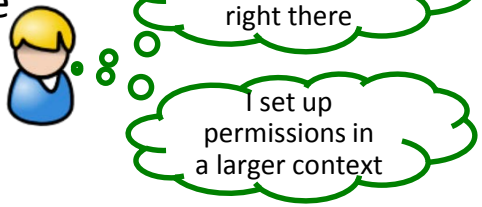
- ✓ Directed

- ✓ Reactive

- ✓ Long-Term

Methods:

- ✓ Concrete
- ✓ Abstract



Controls:

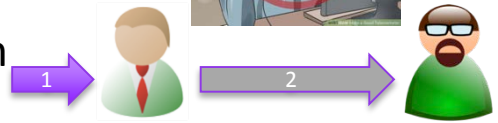
- ✓ Scope

- ✓ Grantee

- ✓ Environment

- Usage

- Downstream



The most robust and strategic option: *lean in to consent*

- Business owners: Engage proactively in regulatory shifts
- Risk teams: Recognize that positive sharing use cases exist
- Business owners: Conceive of personal data as a joint asset
- Go beyond policy to digital transformation “consent tech”

Applying what you've learned

- Next week, find out:
  - Who the **consent stakeholders** are/should be
- By three months, work towards an an **as-built description** of current consent flows against the classification system and analyze:
  - Silos of uncertainty?
  - Consumer trust gaps?
  - Opportunities for directed modes ("delegation")?
- By six months, investigate **opening consent flows** for the classification axes that would make the biggest impact on business goals and compliance posture

RSAConference2017

San Francisco | February 13 – 17 | Moscone Center

SESSION ID: IDY-R03

Thank you!
Questions?

Eve Maler
VP Innovation & Emerging Technology
ForgeRock
@xmlgrrl