



User-Managed Access

Maciej Machulak, PhD

Senior Identity Architect, iWelcome B.V.

maciej.machulak@iwelcome.com / [@mmachulak](https://twitter.com/mmachulak)

Disclaimer

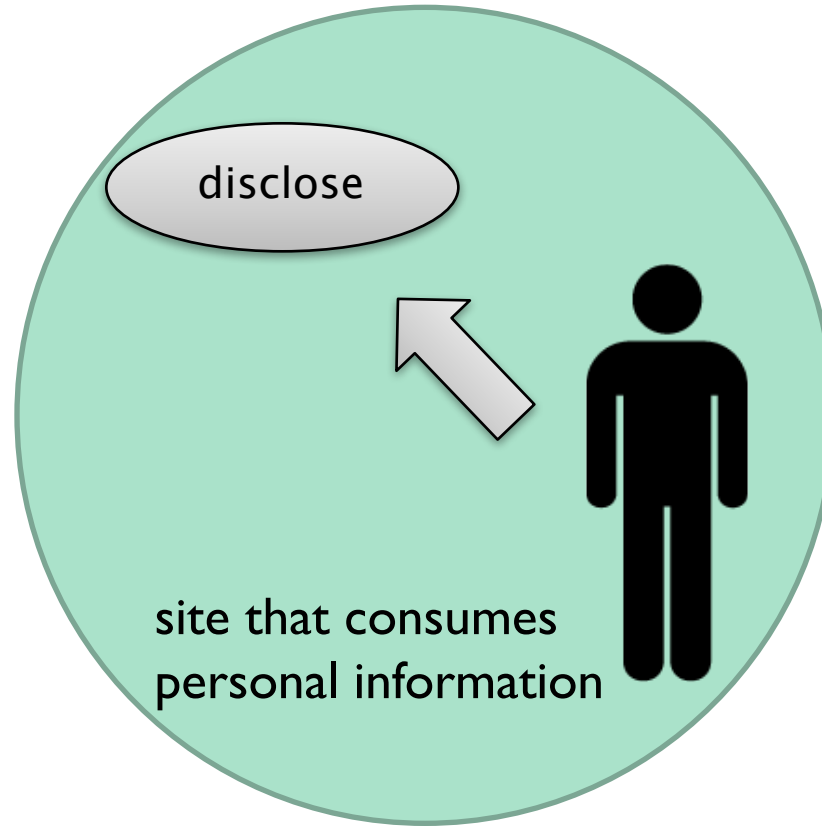
Copyright 2016 iWelcome BV. All rights reserved.

The information in this presentation is provided 'as is' for information purposes only. It does not constitute advice on which you should rely.

This presentation does not constitute an offer to provide any software or services. All third party trademarks, product names, company names and logos appearing in this document are the property of their respective owners, which are in no way associated or affiliated with iWelcome BV. These trademarks, product names, company names and logos have been used for information purposes only.

Sharing Data on the Web

Classic Web 1.0 Model



Classic Web 1.0 Model

- Provisioning user data by hand
- Provisioning it by value
- Oversharing
- Lying!

Name	<input type="text"/>
Street Address	<input type="text"/> <input type="text"/>
City	<input type="text"/>
State	Enter Text <input type="button" value="v"/>
Zip/Postal	<input type="text"/> <input type="text"/>
Province	<input type="text"/>
Country	Enter Text <input type="button" value="v"/>
Phone	<input type="text"/>
Email	<input type="text"/>
Preferred Communication	

Upload Photos to: New Photo Album

Select photos to upload

Clear All

Cancel

No file chosen

No file chosen

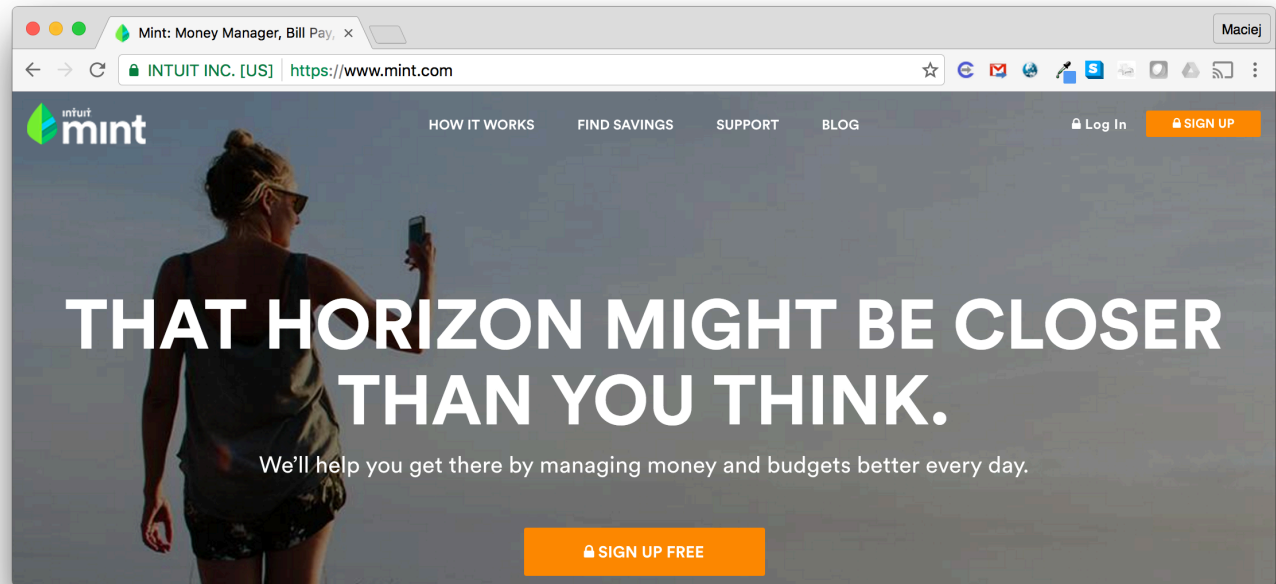
No file chosen

No file chosen

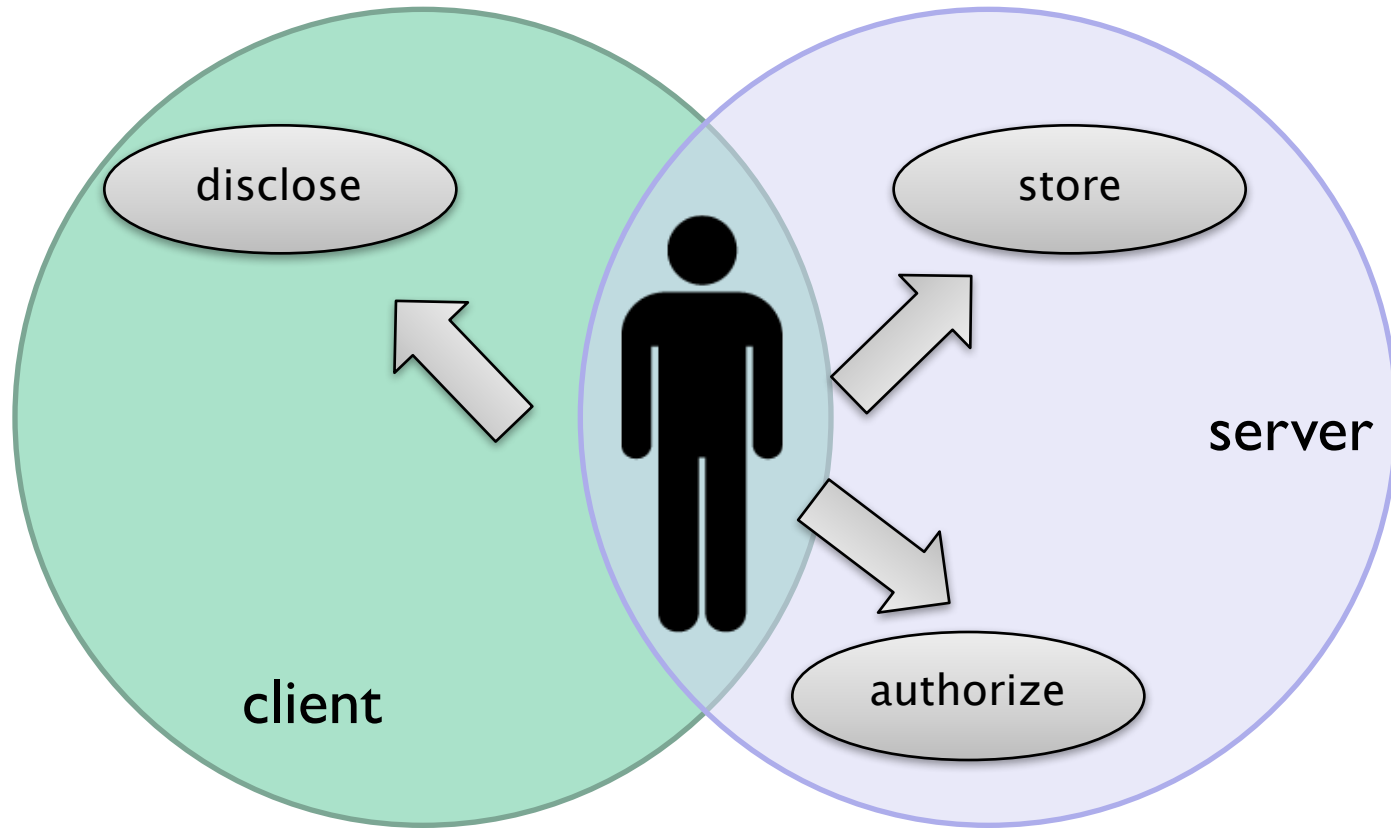
No file chosen

Web 2.0 dark ages for some apps

- “password anti-pattern” - 3rd party impersonates the user
- It’s a honeypot for shared secrets
- B2B partners are in the “gray market”

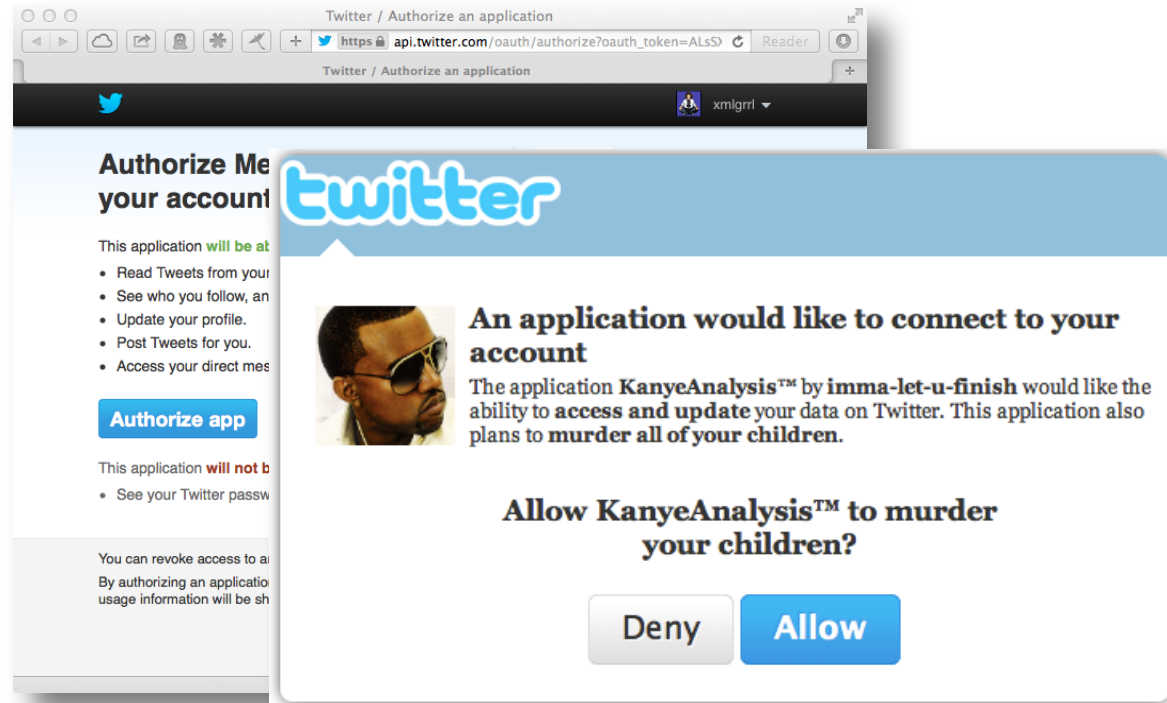


Credit: Eve Maler, ForgeRock Inc.

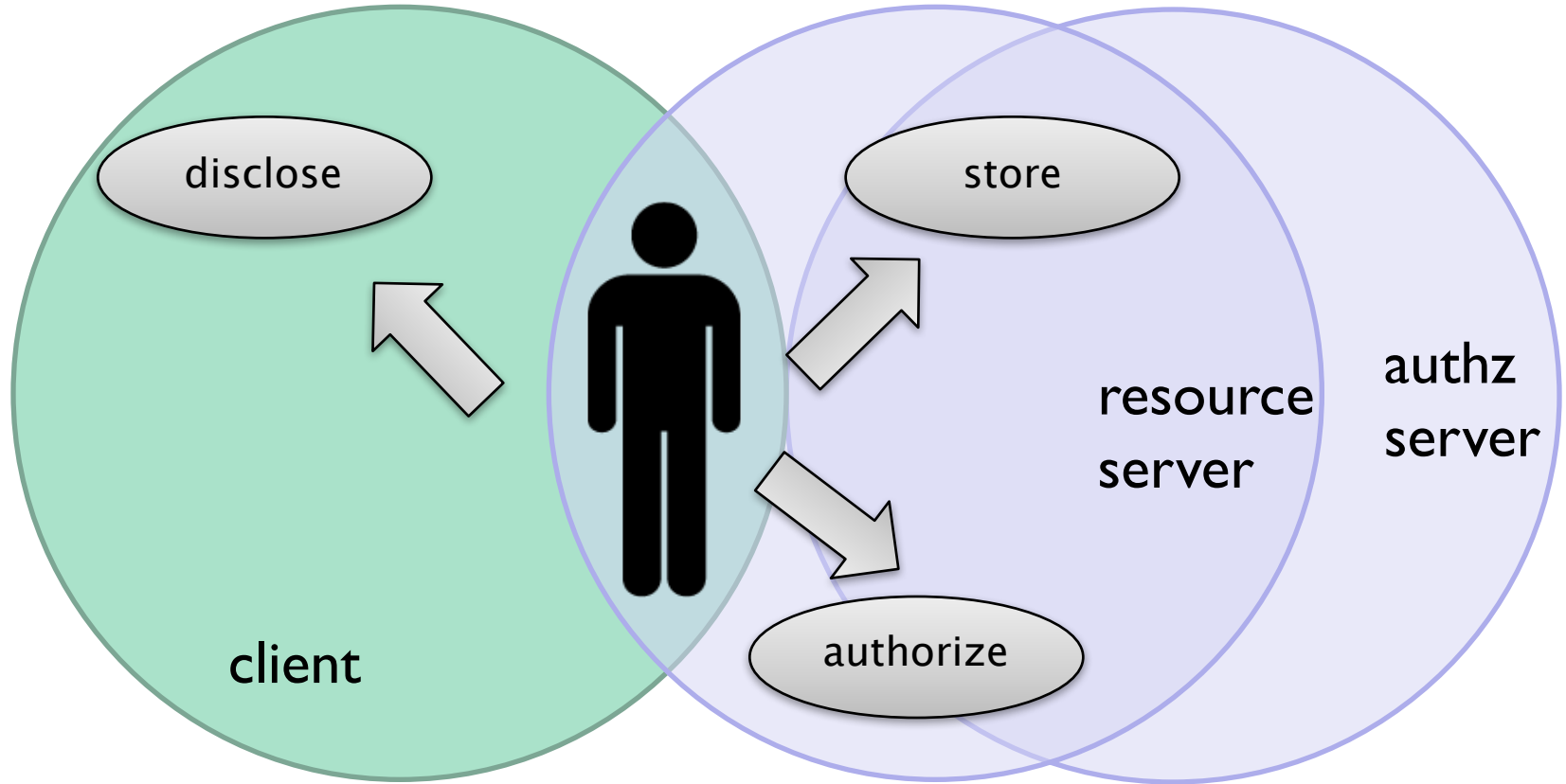


OAuth 1.0/1.0a

- Meaningless consent to unfavorable terms
- Painful, inconsistent, and messy access management
- Oblivious oversharing

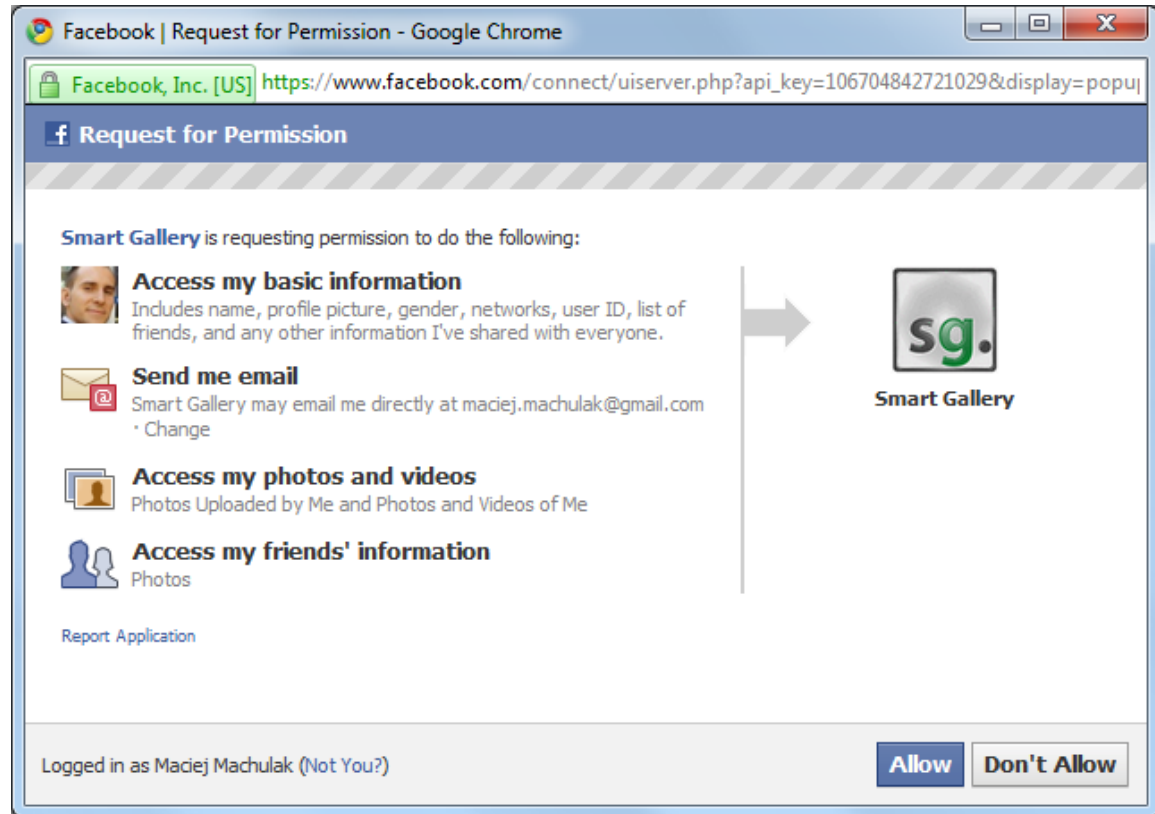


Credit: Eve Maler, ForgeRock Inc.

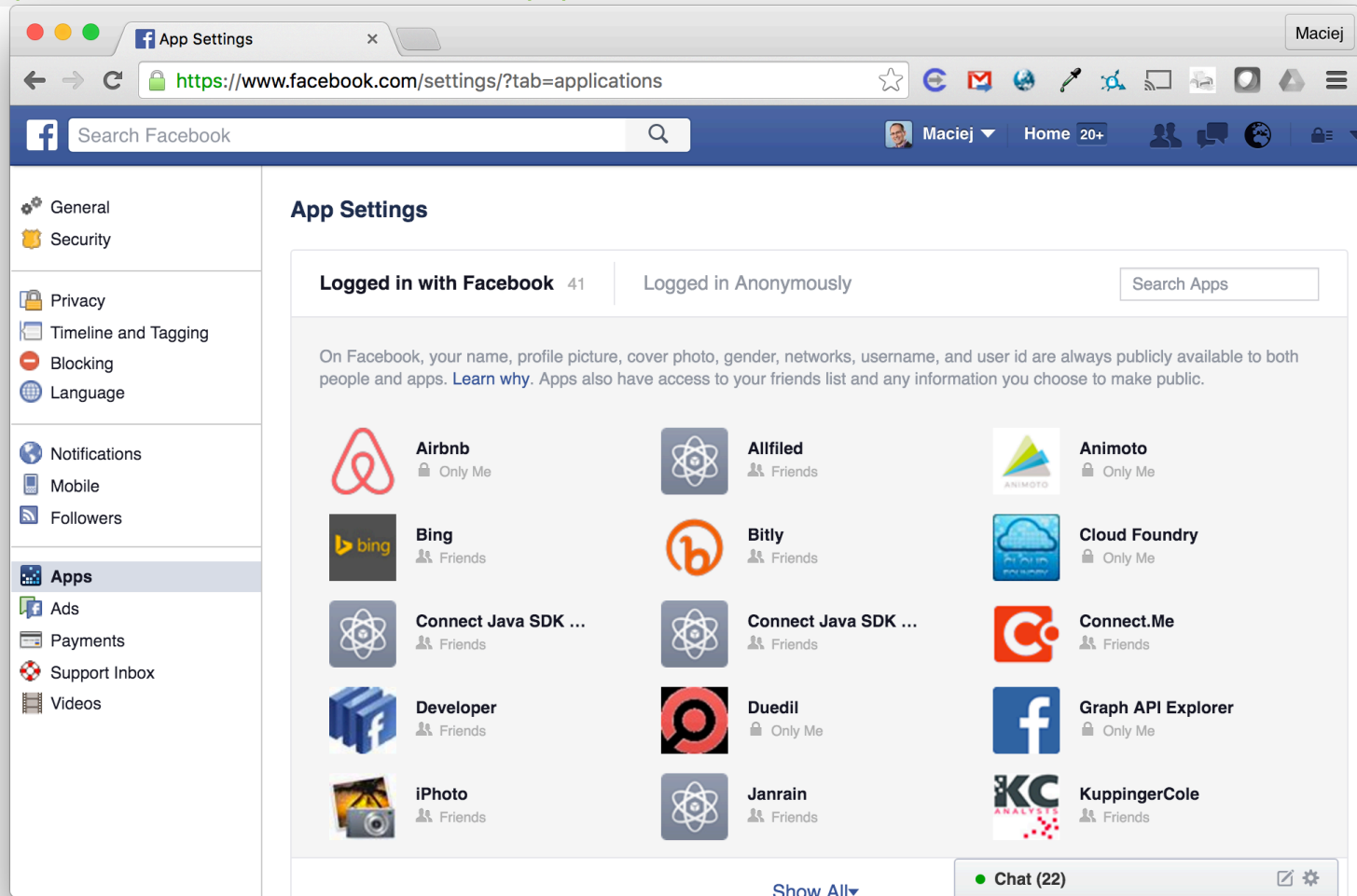


OAuth 2.0

- ...but again we have distributed and hard-to-follow management of security and privacy settings



Application Permissions (I)



The screenshot shows the Facebook App Settings page for a user named Maciej. The page is divided into a left sidebar with navigation links and a main content area. The sidebar includes links for General, Security, Privacy, Timeline and Tagging, Blocking, Language, Notifications, Mobile, Followers, Apps (highlighted), Ads, Payments, Support Inbox, and Videos. The main content area is titled 'App Settings' and shows a list of applications with their permissions. The applications are organized into two columns: 'Logged in with Facebook' and 'Logged in Anonymously'. A search bar is available at the top right of the application list. The applications listed include Airbnb, Bing, Connect Java SDK, Developer, iPhoto, Allfiled, Bitly, Connect Java SDK, Duedil, Janrain, Animoto, Cloud Foundry, Connect.Me, Graph API Explorer, and KuppingerCole. Each application entry shows its icon, name, and the permissions it has access to (e.g., 'Only Me', 'Friends').

App Settings

Logged in with Facebook 41 | Logged in Anonymously | Search Apps

On Facebook, your name, profile picture, cover photo, gender, networks, username, and user id are always publicly available to both people and apps. [Learn why](#). Apps also have access to your friends list and any information you choose to make public.

Application	Permissions
Airbnb	Only Me
Allfiled	Friends
Animoto	Only Me
Bing	Friends
Bitly	Friends
Cloud Foundry	Only Me
Connect Java SDK ...	Friends
Connect Java SDK ...	Friends
Connect.Me	Friends
Developer	Friends
Duedil	Only Me
Graph API Explorer	Only Me
iPhoto	Friends
Janrain	Friends
KuppingerCole	Friends

Show All | Chat (22)

Application Permissions (2)

Twitter / Settings

Twitter, Inc. [US] <https://twitter.com/settings/applications>

Home Notifications Messages Search Twitter

Applications

These are the apps that can access your Twitter account. [Learn more.](#)

You will need to [generate a temporary password](#) to log in to your Twitter account on other devices and apps. [Learn more.](#)

Facebook Connect
Post Tweets to your Facebook profile or page. [Connect to Facebook](#)

Having trouble? [Learn more.](#)

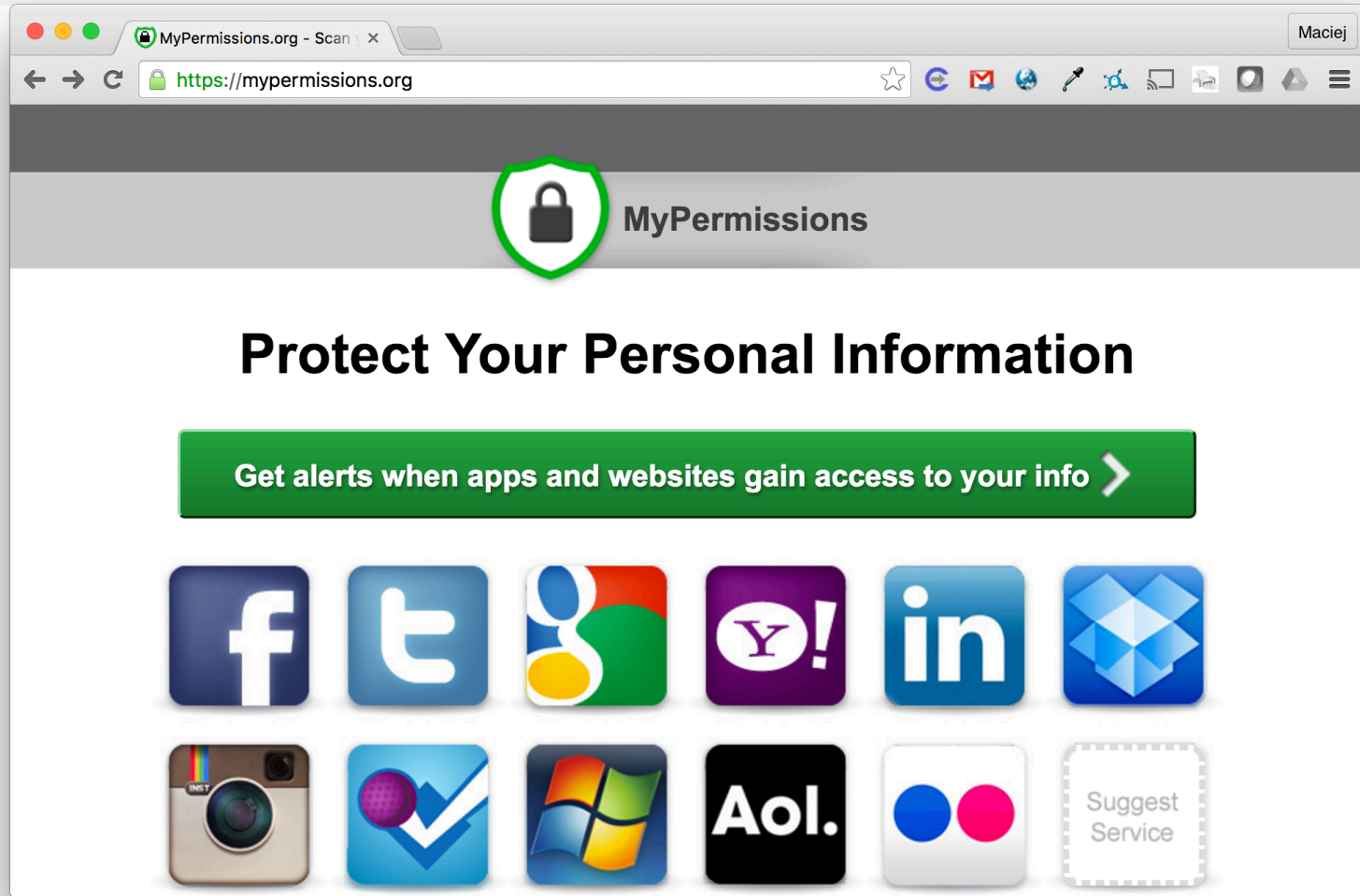
OS X by Apple®
OS X Twitter integration
Permissions: read and write
Approved: Thursday, May 28, 2015 at 11:29:26 AM [Revoke access](#)

Meshfire by Meshfire
Manage your Twitter community with A.I. superpowers.
Permissions: read, write, and direct messages
Approved: Saturday, June 22, 2013 at 6:42:13 PM [Revoke access](#)

Google by Google Inc
Google/Twitter integration.
Permissions: read and write
Approved: Sunday, January 29, 2012 at 11:28:31 PM [Revoke access](#)

NuveAM Demo by Cloud Identity Limited [Revoke access](#)

Account >
Security and privacy >
Password >
Cards and shipping >
Order history >
Mobile >
Email notifications >
Web notifications >
Find friends >
Muted accounts >
Blocked accounts >



Party-to-Party Data Sharing

Vancouver, WA, September 2014


Sep 24 - 26, 2014 / Vancouver, WA

Travelers:

Viewers:

Planners:

Tripit
from Concur



Here Comes the Sun choreo - Google Docs

https://docs.google.com/document/d/1lSWPnKck1K_epT4fTj2EjEWfzEoCKzoOSM8y-BoXU/edit#heading=h.j

Here Comes the Sun choreo - Google Docs

File Edit View Insert Format Tools Table Add-ons Help Last edit was made on August 19, 2013 by Mindy Engelberg

100% Title Trebuchet ... 21 B I U A

1 2 3 4 5 6 7

xmlgrrl@gmail.com

Share

Your account / Allow printing

Flickr has partnered with Snapfish to bring you international printing! You can now use your Flickr photos to make prints, create posters, photo books and more from anywhere in the world.

Who can print your photos

Don't forget to make sure that you have all the necessary rights and you won't be infringing on any third parties with any content that you license on Flickr. As per our [Community Guidelines](#), accounts are intended for members to share content that they themselves have created.

You and your family

flickr

Credit: Eve Maler, ForgeRock Inc.

We can use private URLs...

- Handy but insecure
- Unsuitable for really sensitive data



Credit: Eve Maler, ForgeRock Inc.

...or we can require impersonation...

Import Fidelity Tax Information Into TurboTax®

If you are a Fidelity customer and use TurboTax®, you may be able to import certain information directly from your account into the software. Here's how.

How to import your information

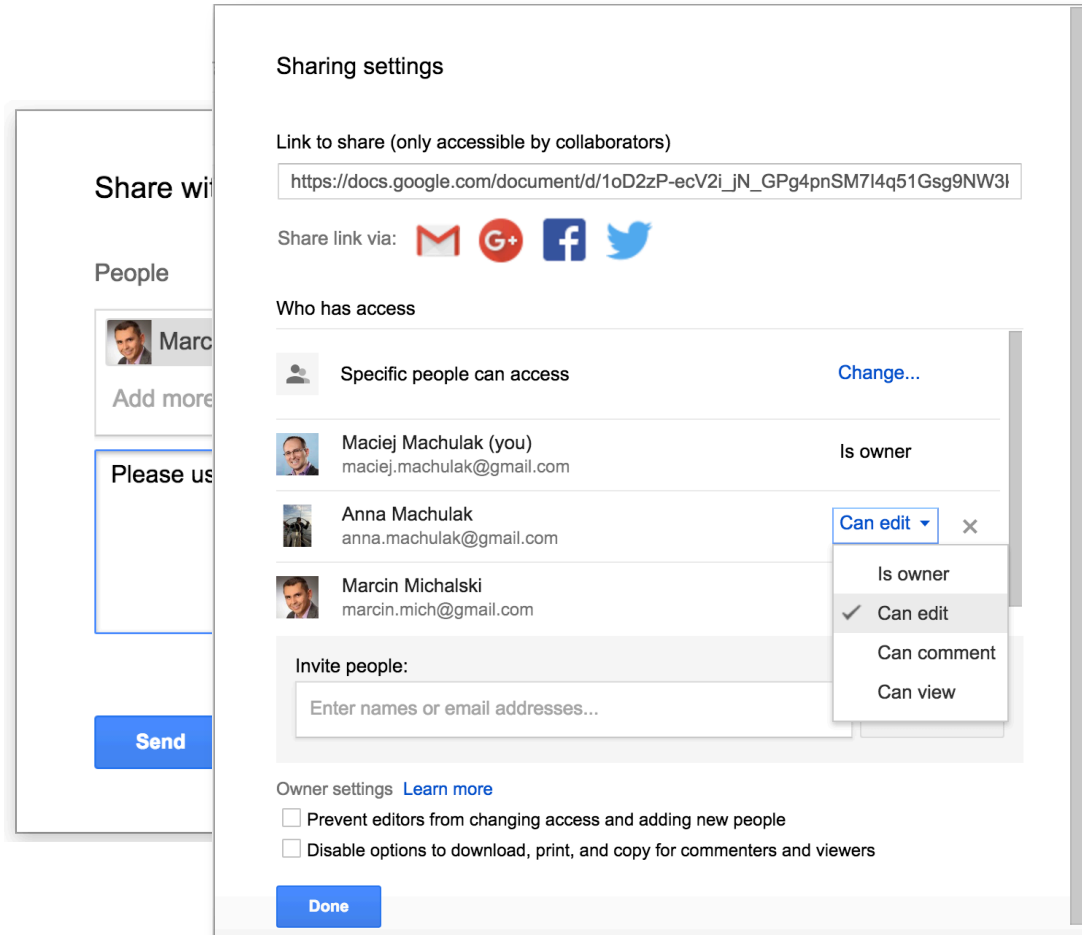
Once you receive your 1099 statement by mail or through eDelivery, have it available to verify the imported information. Follow these simple steps:

1. Enter your Social Security number (SSN), taxpayer identification number (TIN), or username, and then your password. When asked where to import information from, select Fidelity Investments and enter the same information that you use to log on to Fidelity.com. Then, the tax information available for each of the accounts associated with your SSN should appear.

Credit: Eve Maler, ForgeRock Inc.

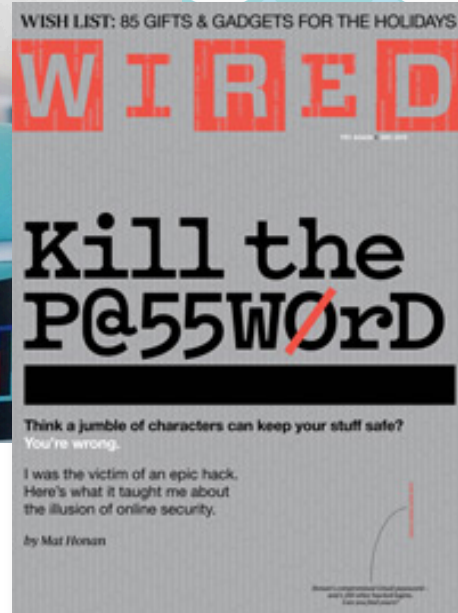
...or maybe...

- ...we can implement a proprietary access management system



Killing – or even wounding – the password kills impersonation

Google's Trust API: Bye-bye passwords. hello biometrics?



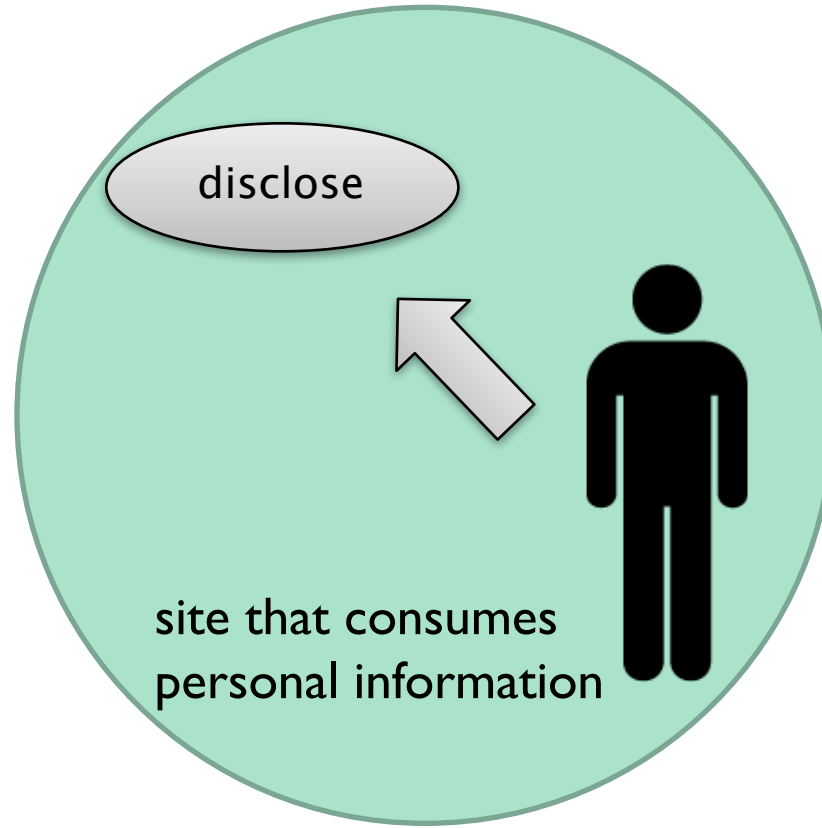
7 Android tools that can help your personal security

Credit: Eve Maler, ForgeRock Inc.

[illegible]

– Gartner Announcement, November 2015

Classic Web 1.0 Model



Terms and Conditions (I)



Source: "Terms and Conditions May Apply", 2013 – <http://tacma.net>



The screenshot shows the top portion of a web browser displaying a TIME News article. The header is a solid red bar with a white menu icon and the word 'TIME' in white serif font. Below the header is a light gray horizontal bar. The article is categorized under 'NEWS' in blue. The title is in large, bold, black sans-serif font. The byline is in a smaller blue font. Below the byline is a row of social sharing buttons: Facebook Share, Facebook Like (with a count of 1.4K), Twitter Tweet, Google+ (with a count of 94), LinkedIn Share (with a count of 155), a red 'Pin it' button, and a gray 'Read Later' button. The first line of the article text is visible at the bottom of the screenshot.

MENU **TIME**

NEWS

You'd Need 76 Work Days to Read All Your Privacy Policies Each Year

By [Keith Wagstaff @kwagstaff](#) | March 06, 2012

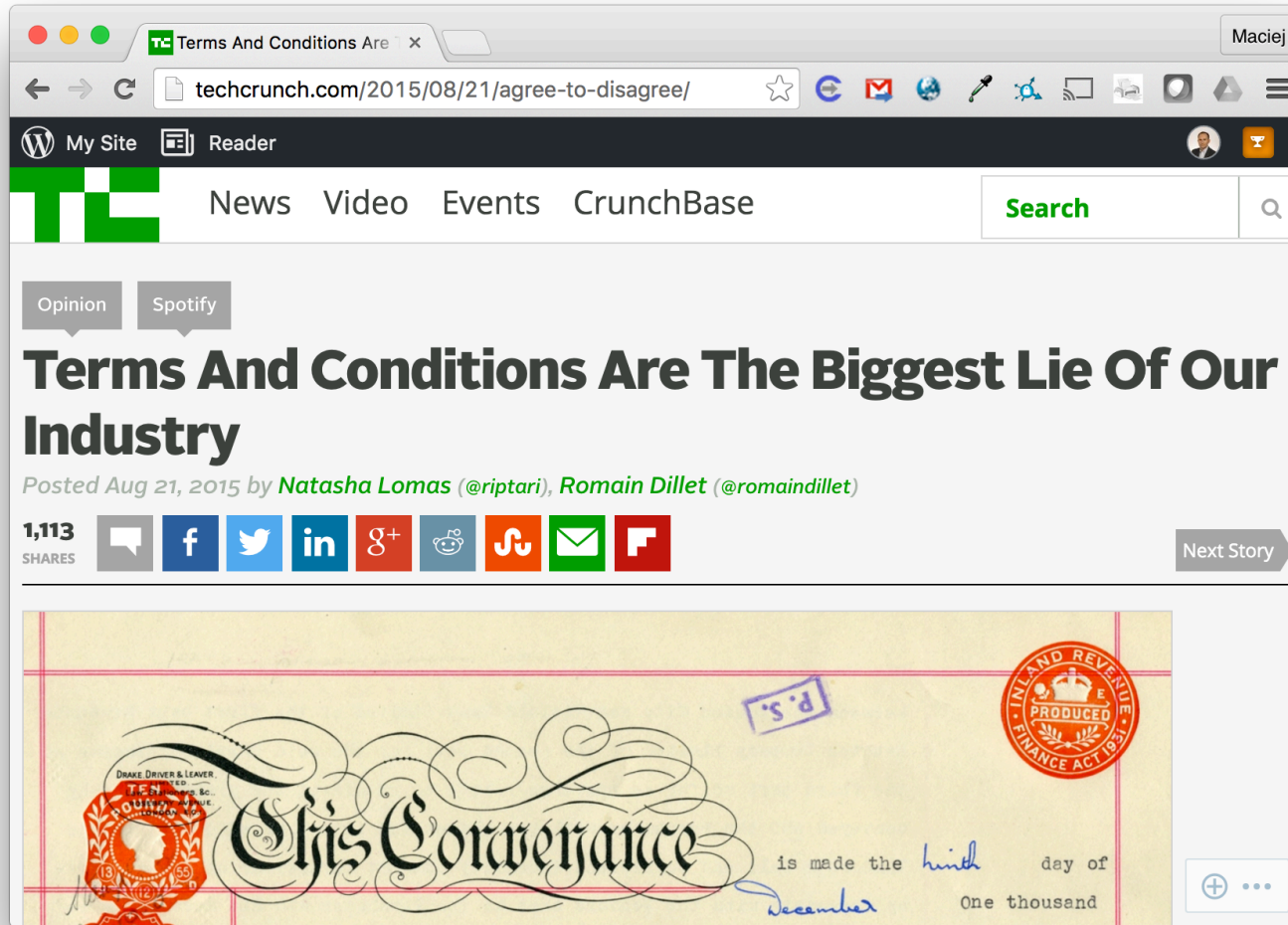
[f Share](#) [f Like](#) 1.4K [t Tweet](#) [G+1](#) 94 [in Share](#) 155 [Pin it](#) [Read Later](#)

The problem with privacy on the Internet isn't so much that companies don't provide privacy

Jose Luis Pelaez Inc / Getty Images

Source: <http://techland.time.com/2012/03/06/you-d-need-76-work-days-to-read-all-your-privacy-policies-each-year/>

Terms and Conditions = Biggest Lie of Our Industry (I)



Source: <http://techcrunch.com/2015/08/21/agree-to-disagree/>

Terms and Conditions = Biggest Lie of Our Industry (2)

“If your business model relies on:

- Misleading your users about your true intentions;
- Obfuscating how much of their data you are sucking up;
- Being as opaque as possible about what you are doing with that data;
- Equivocating on the question of who/what you are selling the data to/sharing it with;

Source: <http://techcrunch.com/2015/08/21/agree-to-disagree/>

Terms and Conditions = Biggest Lie of Our Industry (3)

...continued:

- Intentionally failing to articulate how you are data-mining service usage and user data;
- Not being at all clear about who gets access to the 'insights' you derive from service usage and user data — thereby allowing yourself to claim you don't “sell” any user data

Then you are operating on borrowed time.”

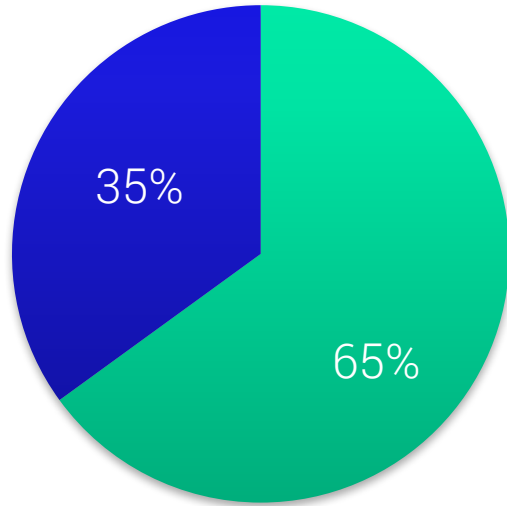
Source: <http://techcrunch.com/2015/08/21/agree-to-disagree/>

„[...] the other biggest lie in the tech industry is that users don't care about privacy.”

Source: <http://techcrunch.com/2015/08/21/agree-to-disagree/>

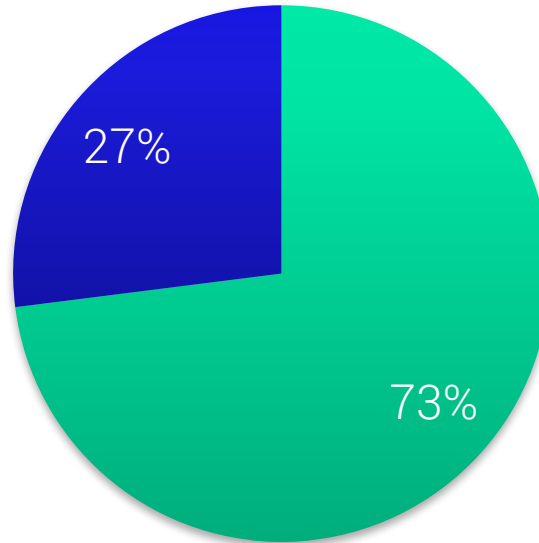
Privacy >> Convenience (I)

Drug prescriptions

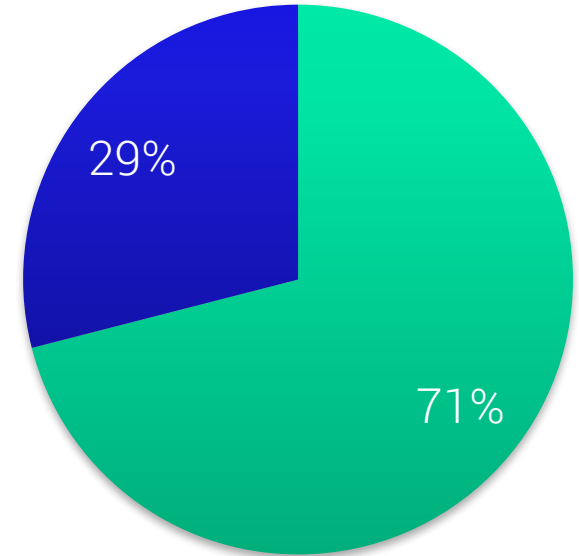


Privacy
Convenience

Doctor's notes



Medical tests



Source: Top health industry issues of 15: Outlines of a market emerge - PwC report, Dec 2014

...same principle applies to virtually any other kind of
personal data...

Source: <http://techcrunch.com/2015/08/21/agree-to-disagree/>

Privacy = Secrecy?



Source: <http://ascom-nuoro.todosmart.net/images/this-privacy.png>

Privacy = Selective Sharing!

General Policies for Patient - 1

Anonymized Analytics Requests

Data Category	Access Decision
Medical Record	<div><div>Allow</div><div></div></div> <div>?</div>
Dietary & Physical Sensor Data	<div><div>Allow</div><div></div></div> <div>?</div>
Psychological Data	<div><div></div><div>Deny</div></div> <div>?</div>

Personalized Analytics Requests

Exceptional Policies

Anonymized Analytics Requests from Organization - 1

Personalized Analytics Requests from Organization - 1

Privacy is not about secrecy

“The goal of a flexible, user-centric identity management infrastructure must be to allow the user to quickly determine what information will be revealed to which parties and for what purposes, how trustworthy those parties are and how they will handle the information, and what the consequences of sharing their information will be”

– Ann Cavoukian, Ontario Information and Privacy Commissioner, Privacy in the Clouds paper



It's about **context, control, choice**, and **respect**

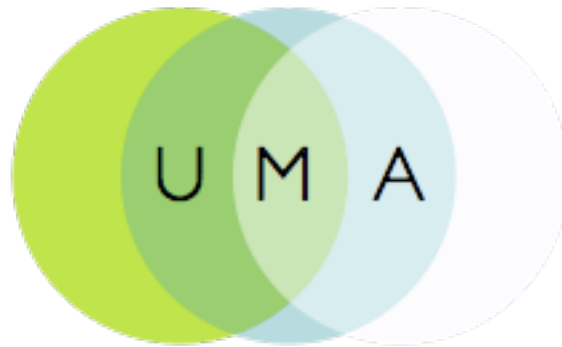
Customers with IDs in digital world need Consent 2.0 solutions

- Context** The right moment to make the decision to share
- Control** The ability to share just the right amount
- Choice** The true ability to say no and to change one's mind
- Respect** Regard for one's wishes and preferences



Credit: Eve Maler, ForgeRock Inc.

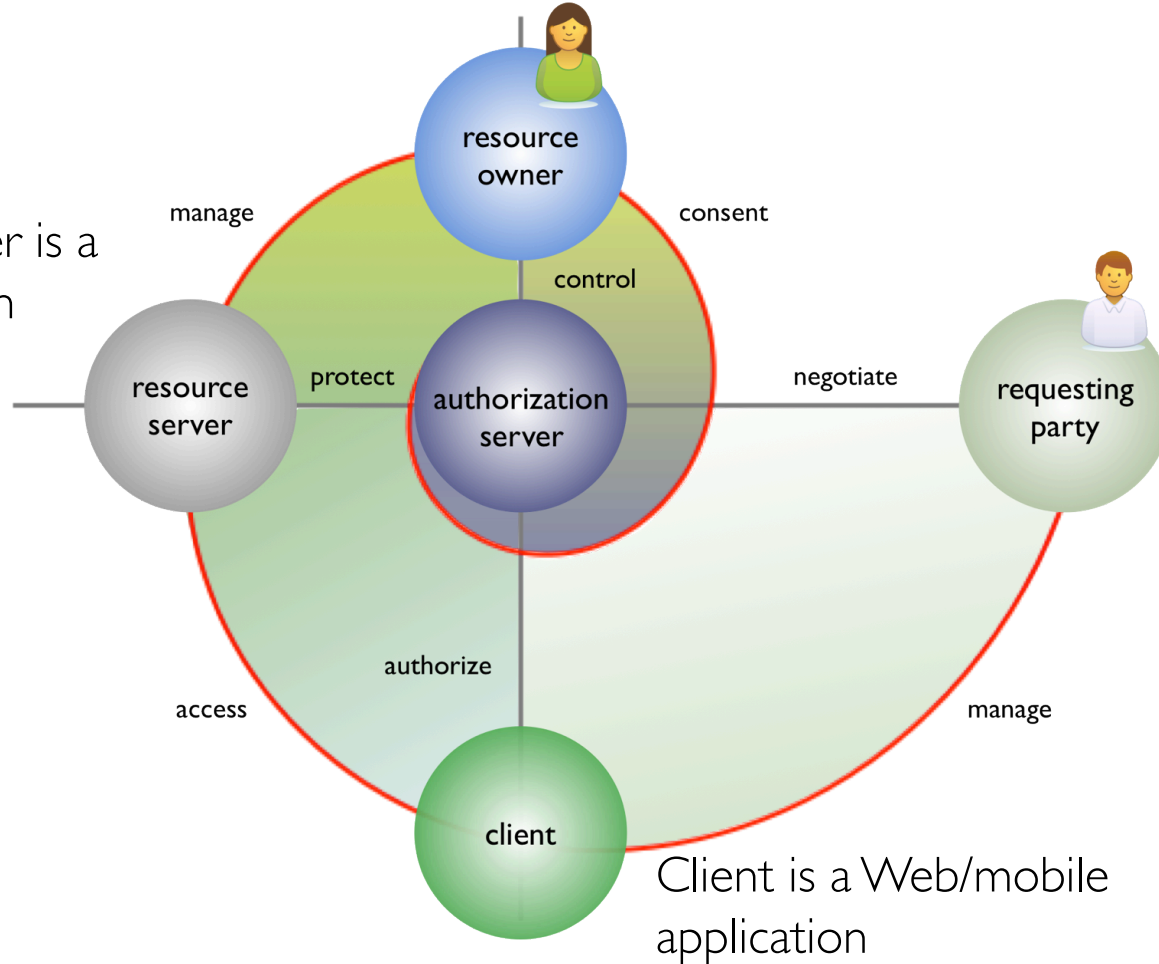
UMA to the rescue!

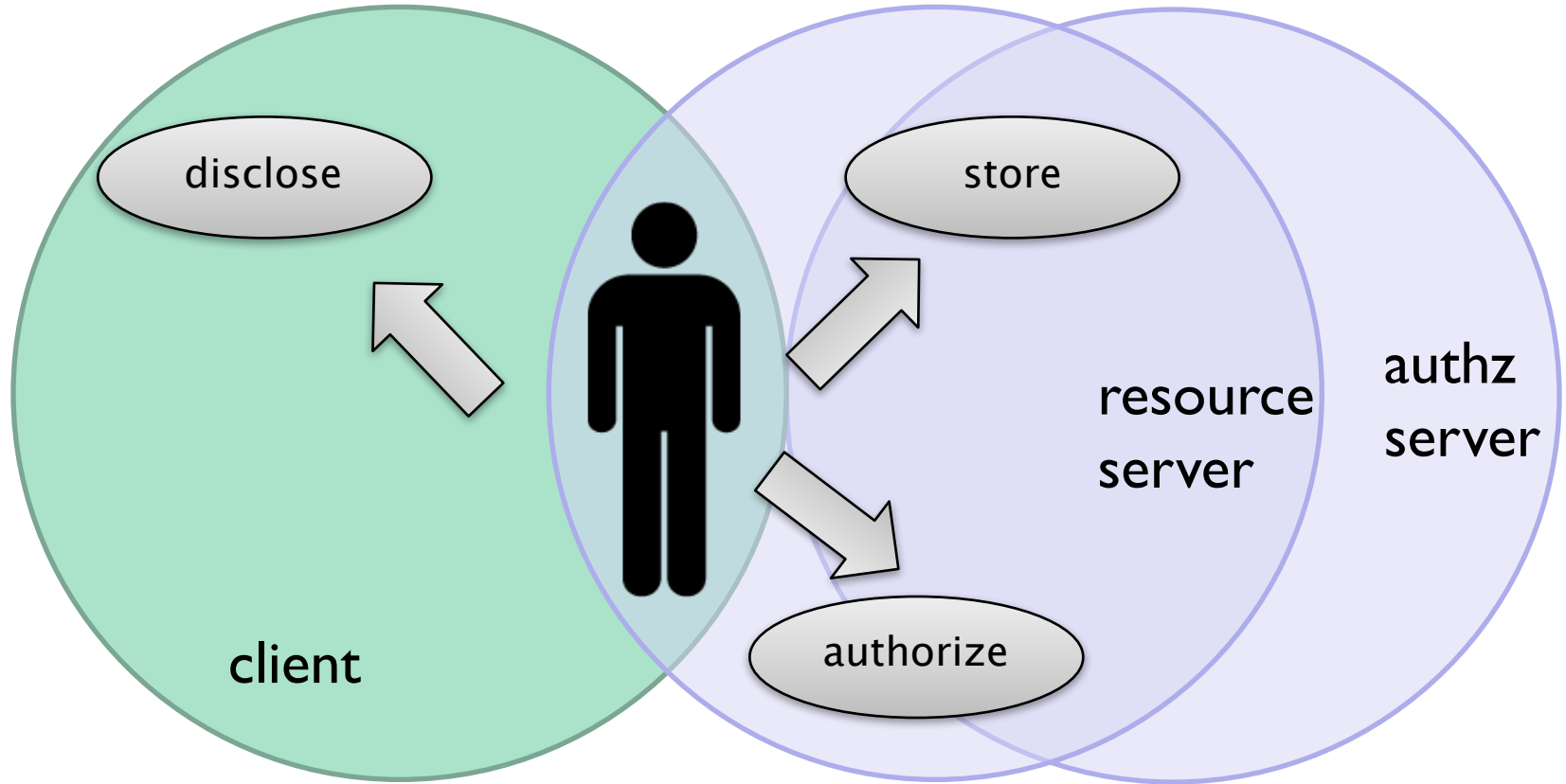


User-Managed Access (UMA) is a profile of OAuth 2.0. UMA defines how **resource owners** can **control** protected-resource **access** by **clients** operated by arbitrary **requesting parties**, where the **resources** reside on any number of **resource servers**, and where a centralized **authorization server** governs access based on resource owner **policies**.

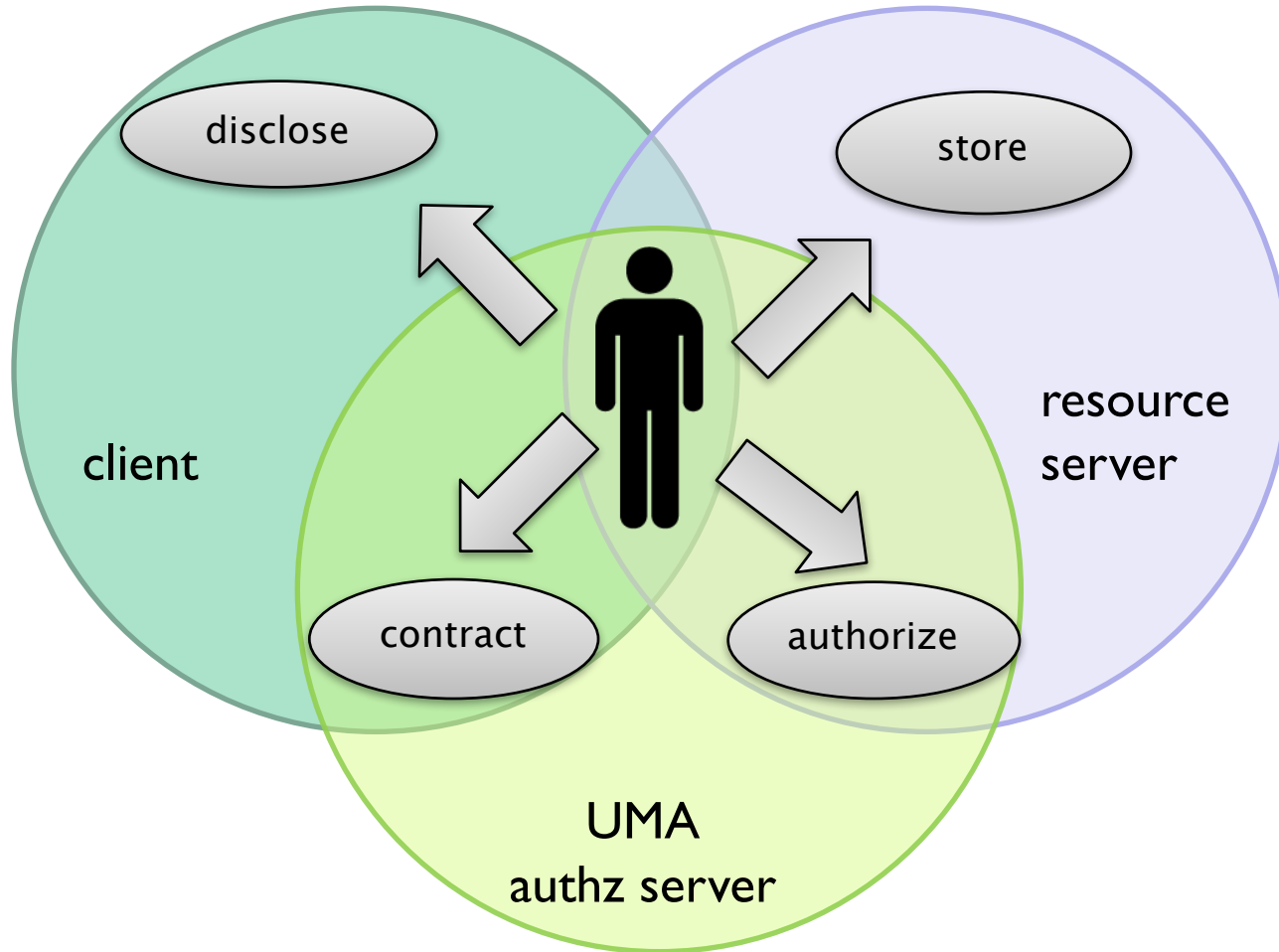
UMA Architecture

Resource Server is a
Web application

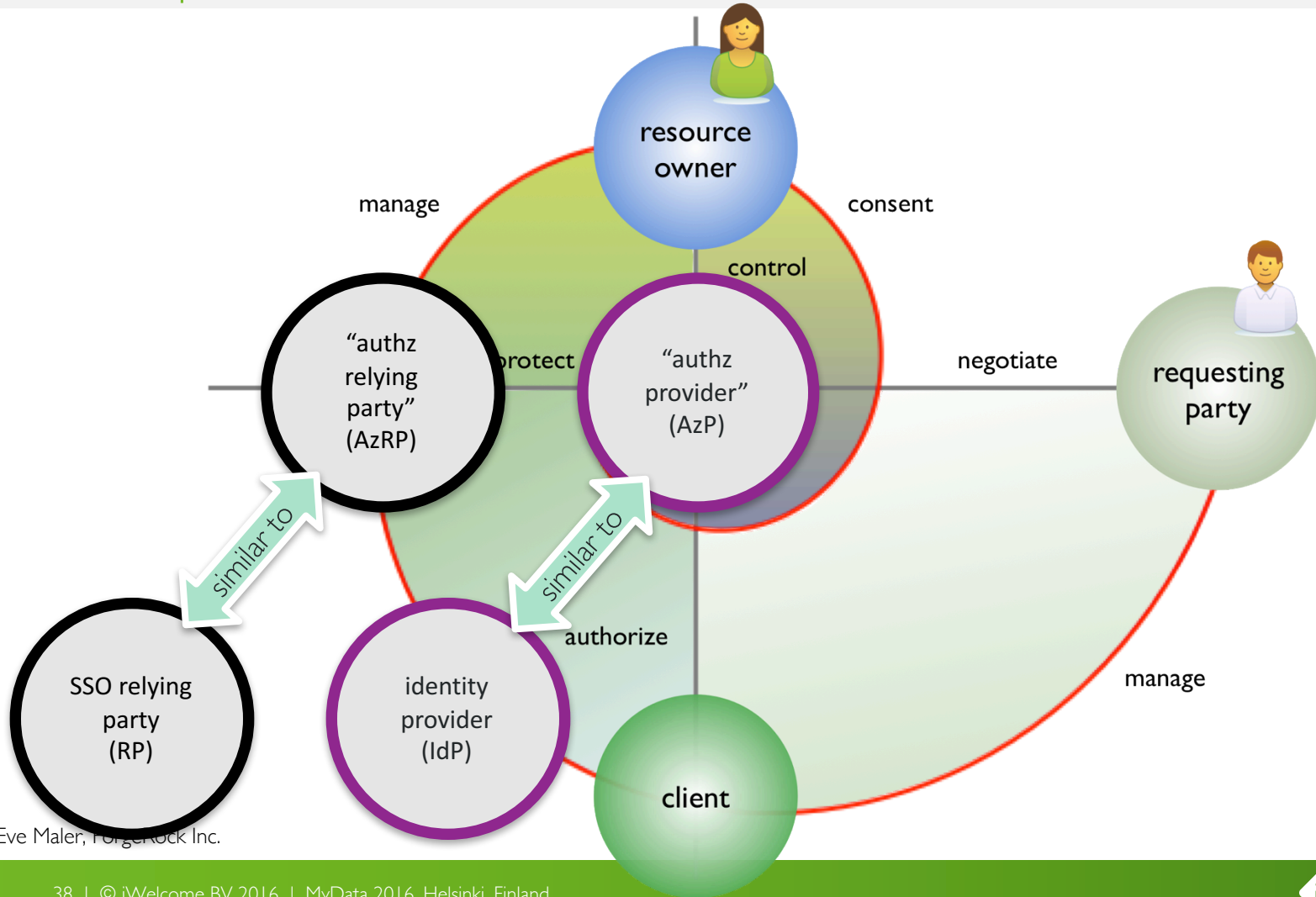




User-Managed Access (UMA)



Interoperable, RESTful authorization-as-a-service

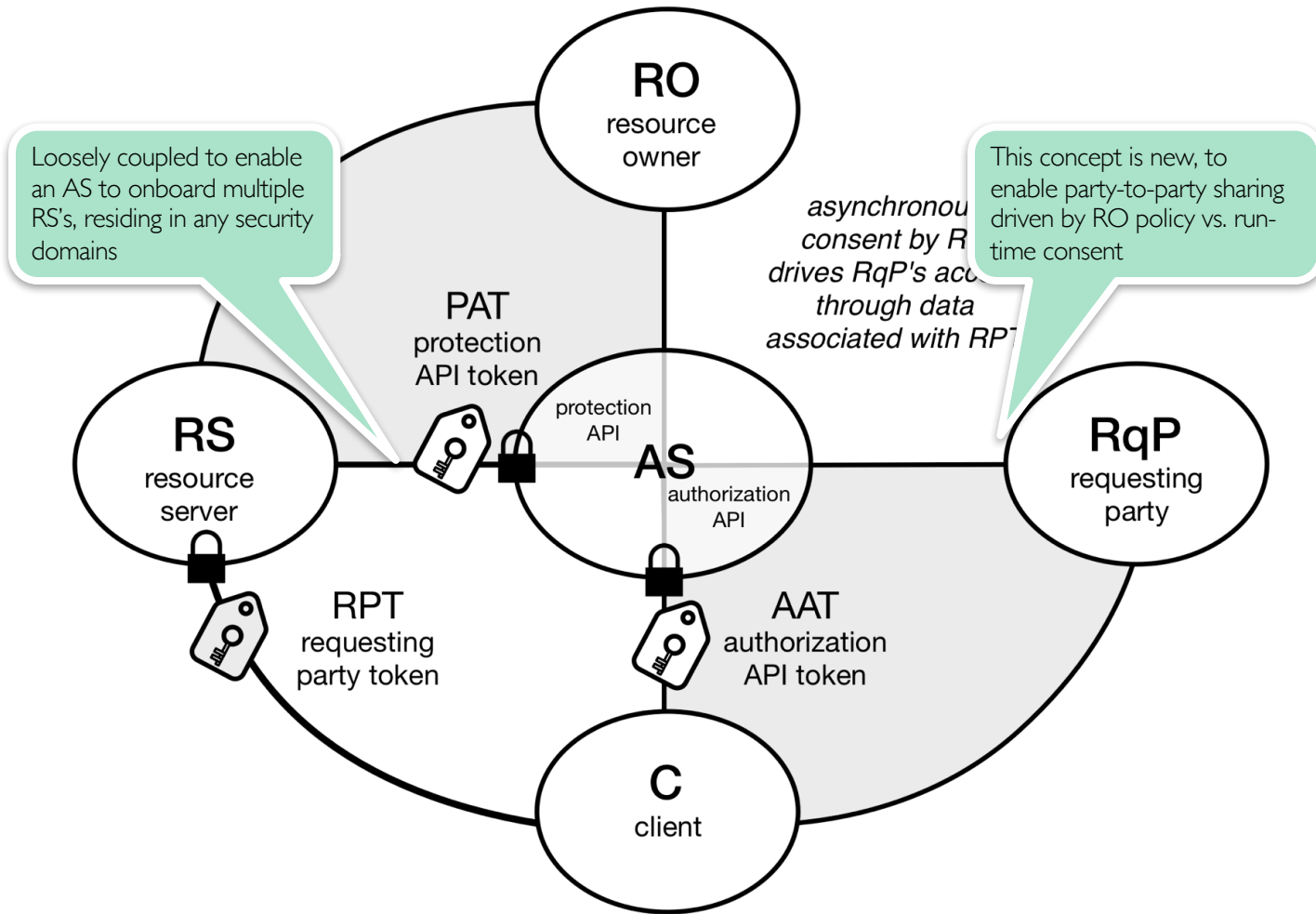


Credit: Eve Maler, ForgeRock Inc.

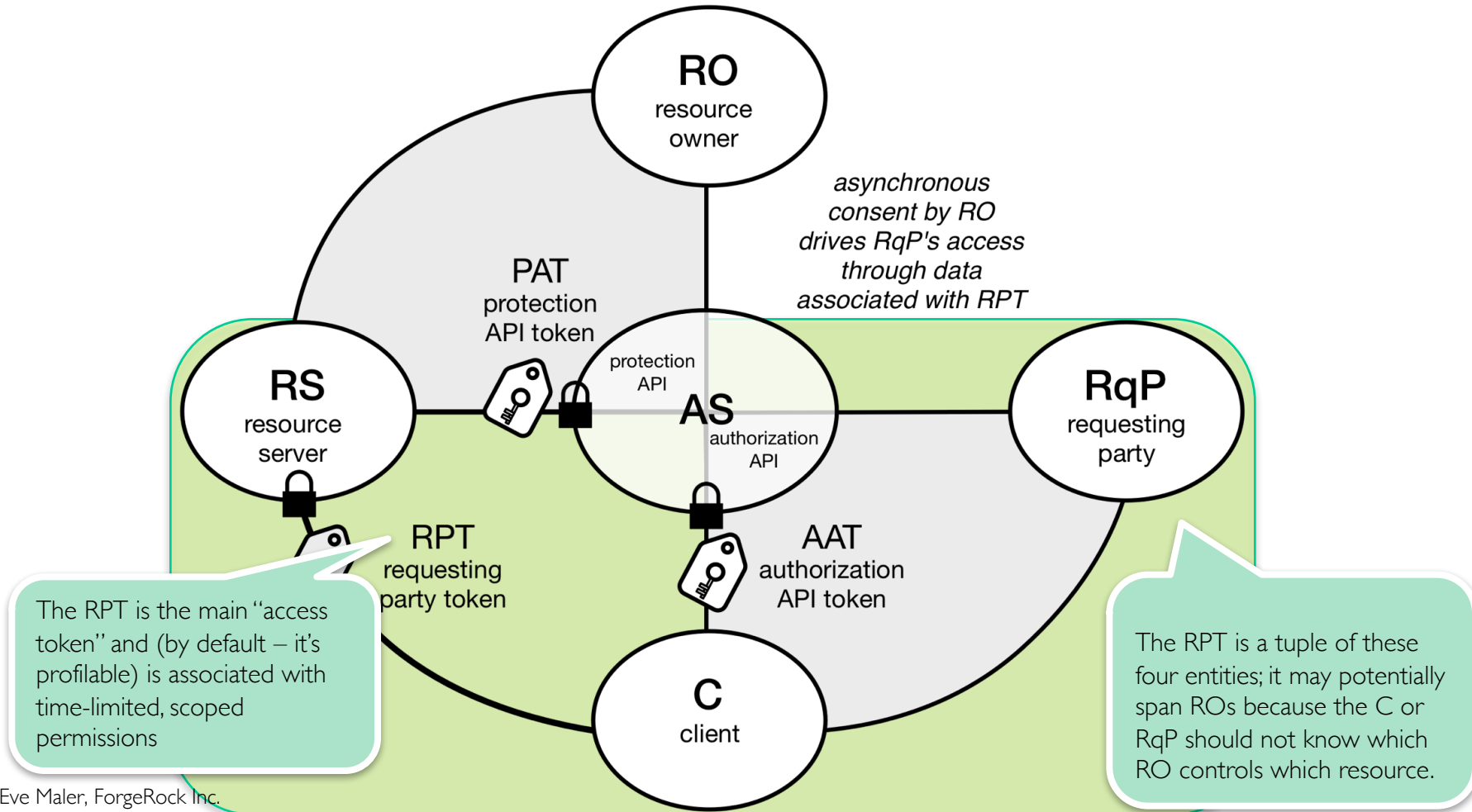
Example policy types suitable for UMA

- Share with bob@gmail.com
- OK to read but “do not print”
- Only for those > 18 years old
- If member of ACME University

Under the hood, it's "OAuth++"

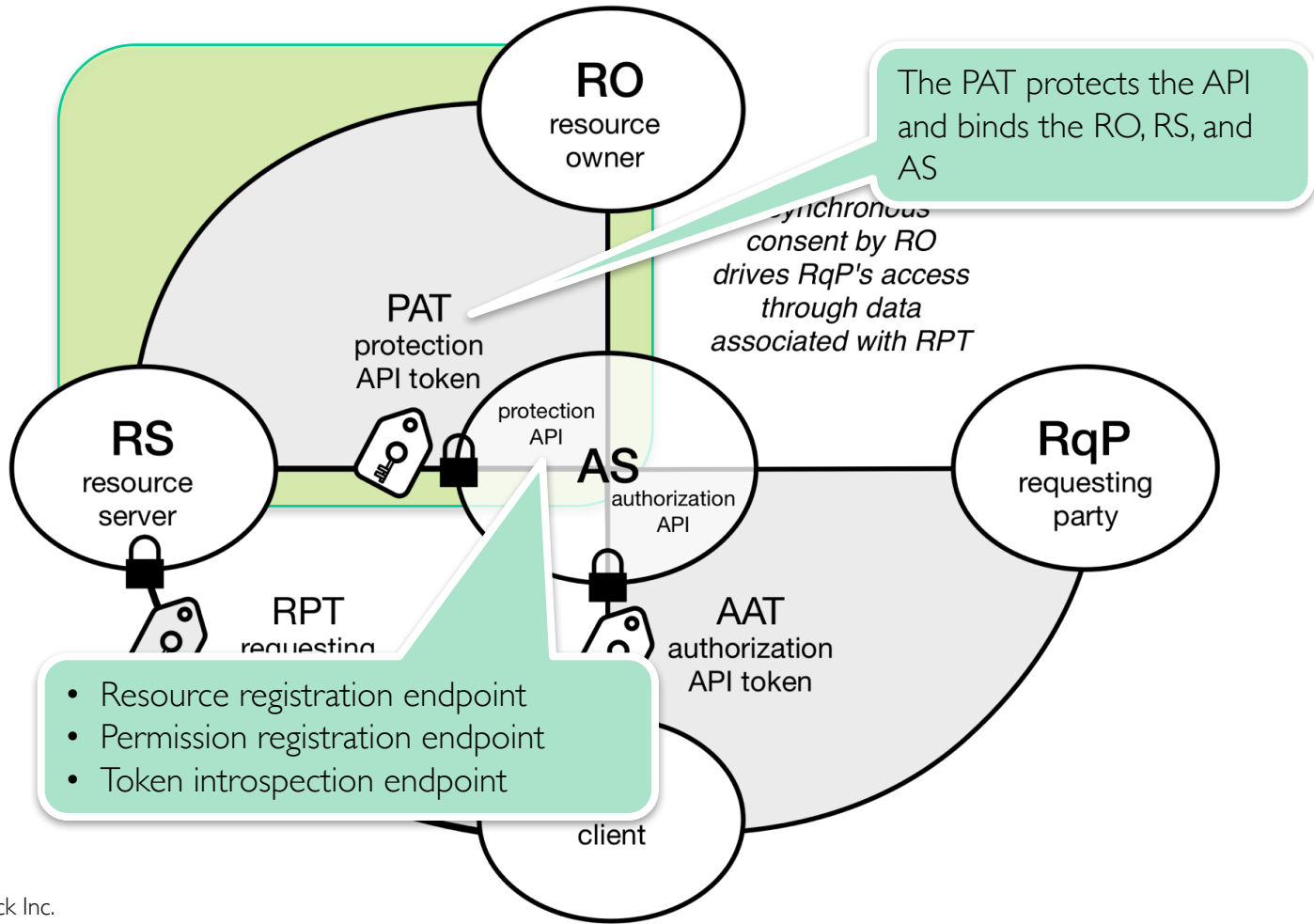


Under the hood, it's “OAuth++”



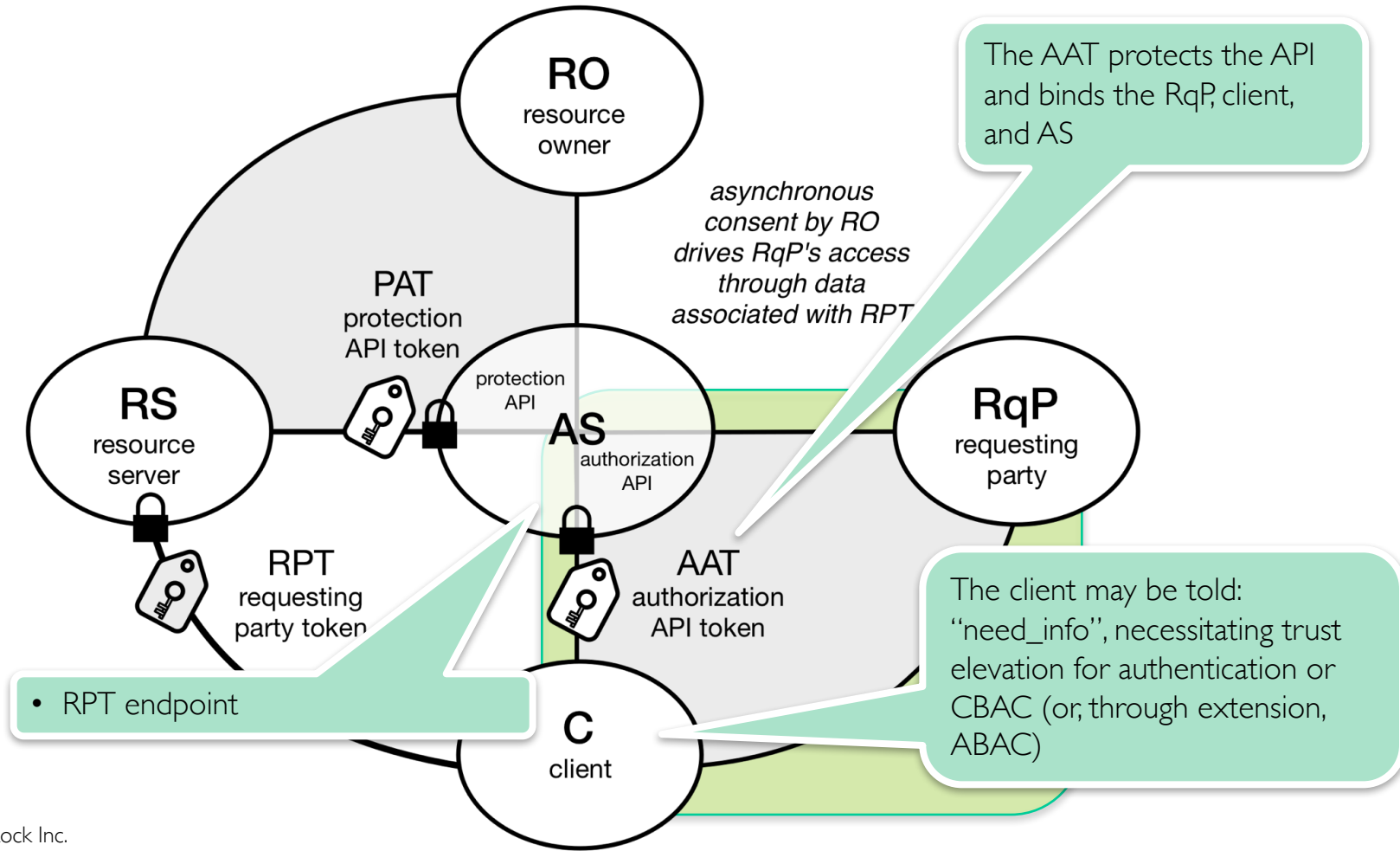
Credit: Eve Maler, ForgeRock Inc.

Under the hood, it's "OAuth++"



Credit: Eve Maler, ForgeRock Inc.

UMA authorization API for the Client



Credit: Eve Maler, ForgeRock Inc.

Embedded OAuth flows to protect UMA security APIs

- The **PAT** and **AAT** are names for plain old OAuth tokens
 - representing important UMA concepts!
 - **PAT** = Alice's consent to federate authorization
uma_protection OAuth scope
 - **AAT** = Bob's consent to share claims to get access
uma_authorization OAuth scope

UMA SUMMARISED

- It's a protocol for lightweight access control
- It's a profile and application of OAuth2
- It's a set of authorization, privacy, and consent APIs
- But also... it's a Kantara Initiative Work Group
- And it's already made up of two recommendations (standards)
 - V1.0
 - V1.0.1
- Under further development towards V2.0(?)

- User-Managed Access (UMA) specifications
 - UMA V1.0 - April 2015
 - OAuth 2.0 Resource Set Registration - April 2015
 - UMA V1.0.1 – December 2015
 - OAuth 2.0 Resource Set Registration - December 2015
- UMA Claims-Gathering Extension for Enhanced Security – March 2016

Upcoming UMA changes (I)

- UMA is being under further development
 - but existing V1.0.1 is already ready for deployment!
- Alignment with OAuth 2.0 and OIDC protocols
 - to simplify adding UMA in existing OAuth/OIDC deployments
- Incorporation of ticket rotation
 - adopted from UMA Sec Ext (lessons from OAuth 1.0a)
- Syntactical changes
- Serving more use cases: wide vs narrow ecosystem, IoT (see IETF ACE WG)

Upcoming UMA changes (2)

- UMA WG also works further on (possibly) breaking changes
 - aiming for V2.0
- These potential changes (not yet approved) include:
 - Removal of AAT
 - Removal of RPT endpoint

UMA Deep Dive and Details

- Need more information on UMA?
 - reach out to me after this talk
 - ...or during the breakout sessions!
- Real working implementation of the UMA protocol:
 - “Transcript of Records Sharing Scenario”
- Sign-up for the UMA WG at Kantara Initiative
 - ...and follow @UMAWG on Twitter!



Thank you for your attention!