Extending the Power of Consent with User-Managed Access

A Standard Architecture for Asynchronous, Centralizable, Internet-Scalable Consent

Eve Maler, ForgeRock
eve.maler@forgerock.com
@xmlgrrl
May 21, 2015

"Privacy" goals vs. reality

- **Aspirations:** FIPPs and Privacy by Design speak of transparency, control, participation, consent…
- **Risk mitigation:** The top driver for corporate privacy funding is meeting compliance obligations
  - >50% of corporate and government privacy groups report into Legal or Compliance
- **Ready for a change?** 91% of Americans agree or strongly agree consumers have lost control over PII collection and use
  - 80% who use social networking sites are concerned about third-party access

In ordinary online contexts, the consent experience is dire
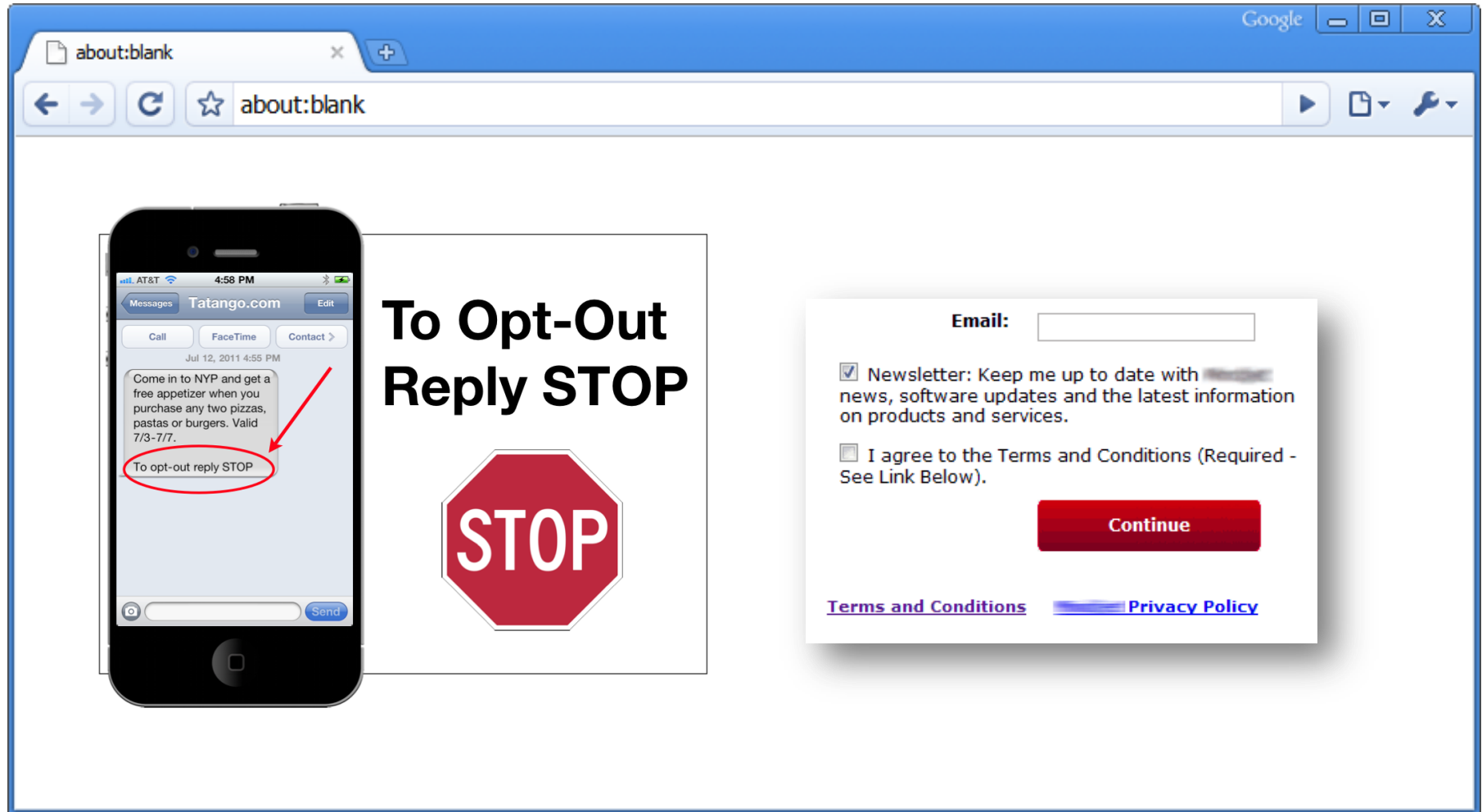
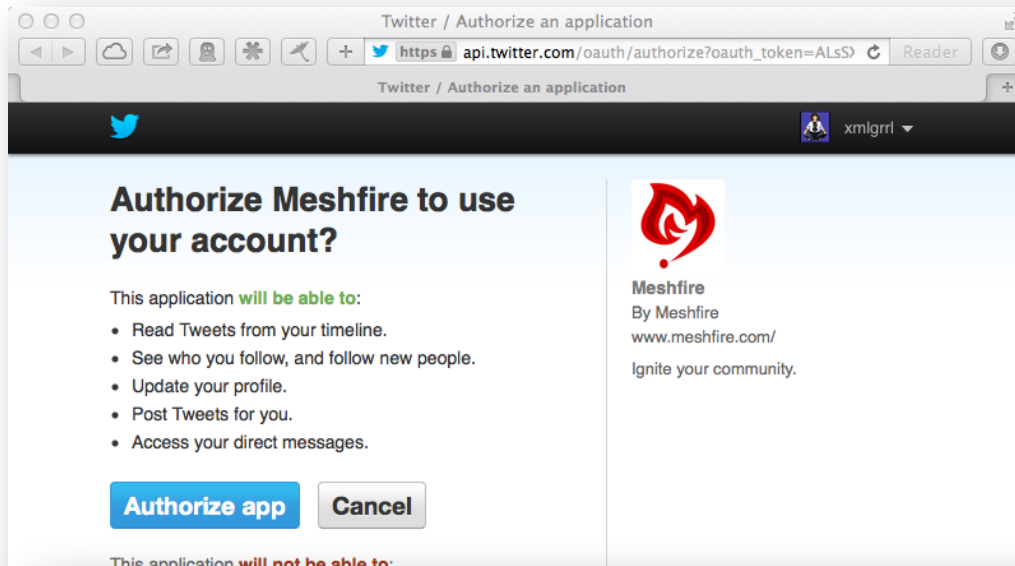# In the Internet of Things, it's not going to get easier

The Next Step in Wearable Electronics

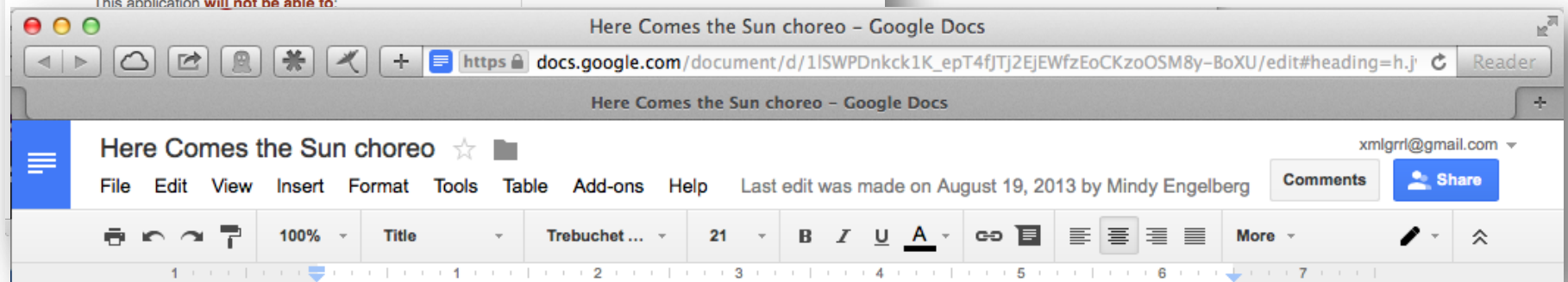By Julia Goldstein on May 4 2015 // No Comments

A funny thing happened in the API economy: beyond-compliance consent paradigms

OAuth opt-in consent for scoped API access

Directed scoped sharing with other people

Consent requirements that freshen up our aspirations

Choice

authorization   agreement   acquiescence

Relevance

☑ **Time**   ☑ **Manner**   ☑ **Consciousness**

Granularity

☑ **Sources**   ☑ **Data items**   ☑ **Parties**   ☑ **Modification**

Scalability

☑ **Sources**   ☑ **Data items**   ☑ **Consent interactions**

Automation

☑ **Processing**   ☑ **Recording**

Reciprocity

Consent of resource owner to share

Consent of requesting party to be recognized
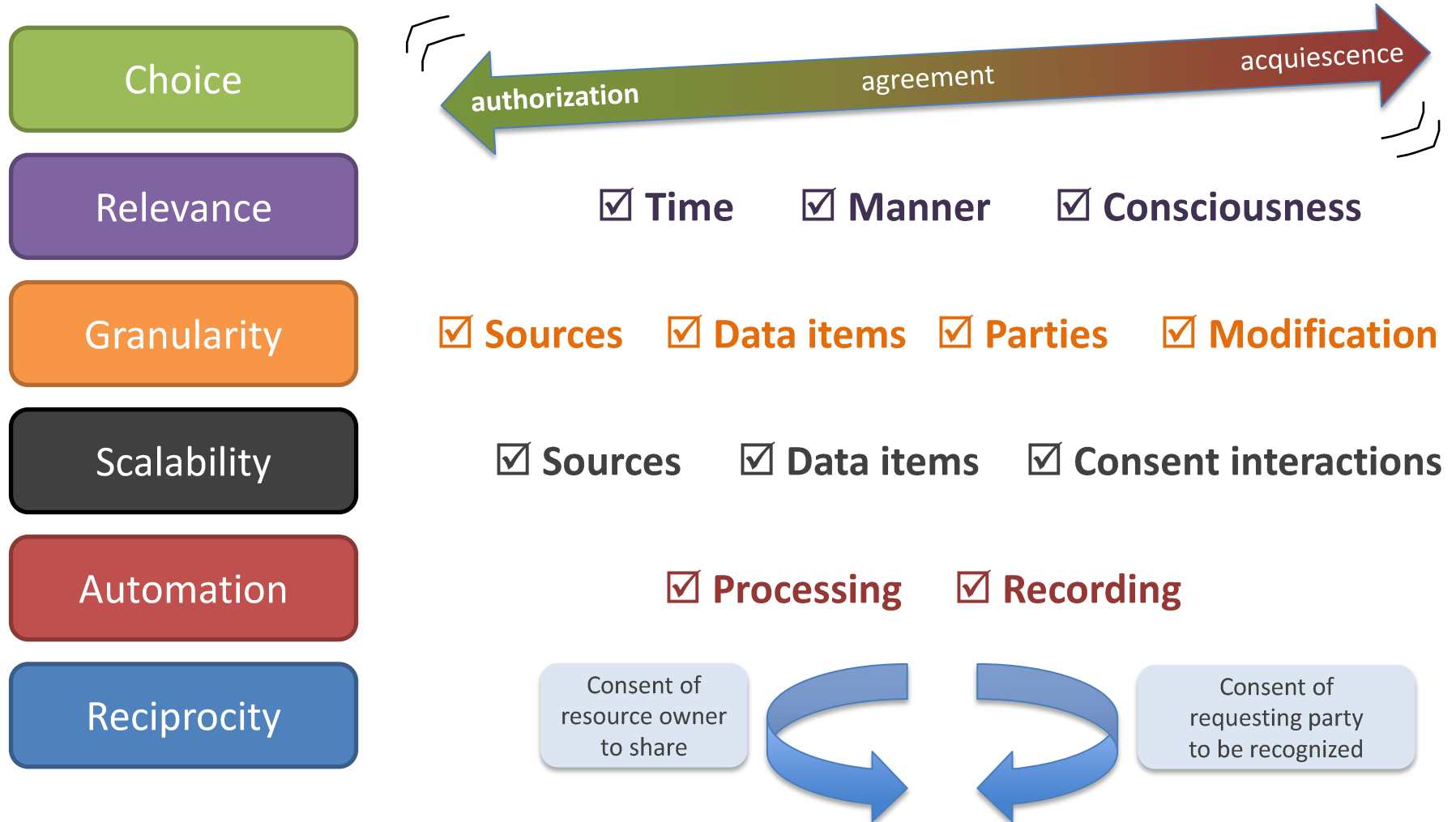
How do classic and new consent mechanisms do against the requirements?

The paper thing at the doctor's office

	ToS opt-in	Cookie opt-in/out	OAuth	"Share"	Consent directive
Choice	-1	0	0	+1	+1
Relevance	-1	0	+1	+1	0
Granularity	-1	0	0/+1	+1	0
Scalability	-1	+1	0	-1	-1
Automation	-1	0	+1	+1	-1
Reciprocity	-1	-1	-1	0	-1

The User-Managed Access (UMA) V1.0 standard builds on OAuth, and adds "Share" features

Loosely coupled to enable centralized authorization-as-a-service for any number of an individual's resource servers

A new concept, to enable party-to-party sharing driven by policy (or access approval) rather than requiring the individual to be present at access time

Authorization data is added to this token if trust in the requesting party is successfully elevated, typically through authentication and/or claims-gathering

RO resource owner

RS resource server

AS authorization API

RqP requesting party

C client

PAT protection API token

protection API

RPT requesting party token

AAT authorization API token

asynchronous consent by RO drives RqP's access through data associated with RPT

https://himss.openrock.org:8043/openam/XUI/#uma/resources/

UProtect

☐ Dashboard   ☐ **Shares**

☐ Alice Henderson ▾

Resources   History

Resources ☐

☐ Revoke All

🔍 Filter by Resources

Resources	**Host**	**Type**
⮜ **Allergies**	BlueHealth	https://bluehealth.openrock.org:443/types/medical
⮜ **Allergies**	BlueHealth	https://bluehealth.openrock.org:443/types/medical
⮜ **Heartrate**	HappyHeart	https://happyheart.openrock.org:443/types/medical

« ‹ 1 › »

info@forgerock.com
Copyright © 2010-15 ForgeRock AS, all rights reserved.

How does UMA do against the requirements?

	UMA
Choice	0/+1
Relevance	+1
Granularity	+1
Scalability	0/+1
Automation	0/+1
Reciprocity	+1

Thank you

Eve Maler, ForgeRock
eve.maler@forgerock.com
@xmlgrrl
May 21, 2015