USER-MANAGED ACCESS: USE CASES FOR ANALYZING AND DETERMINING A LEGAL FRAMEWORK

By

Timothy Reiniger

(2/28/17)

(as edited according to UMA Legal Subgroup instructions 3/26/2017)

I. *Lex Informatica* Considerations

A. UMA Value Proposition for Programmable Devices, Network Systems, and Applications
   1. Consumer Access Control (Autonomy)
   2. Trusted Relationships (Reciprocity)
   3. Default Rules/Policies (Objectivity)

B. UMA Consent Advantages
   1. Diachronic Consent/Access Control (information is being added and changed over time)
   2. Asynchronous Consent/Access Control
   3. Delegated/Distributed Authorization Chain

C. UMA Legal Advantages
   1. Jurisdictional: Networks and Cross-Border Interoperability
   2. Customization of Consumer Control over Access Rights/Permissions
   3. Self-Enforcement: Monitoring and *Ex Ante*

D. UMA Legal Challenges
   1. Data Ownership – How Does the Consumer Gain Access Control?
   2. Device Function Control – Who Controls?
   3. Identity and Authorization of RqPs
   4. Downstream Control and Monitoring of Personal Information Access, Distribution, and Use Rights
   5. How enforce access controls and authorizations/permissions?

II. Salient Factors for Use Cases

A. Networked-Access Environments
   1. Consumer-Facing Smart, Connected Products
   2. Consumer-Facing Mobile Phone Applications
   3. Consumer-Facing Online/Cloud Applications
   4. Employee-Facing in Enterprise
   5. Citizen-Facing Government Services
   6. Regulated Access Rights/Duties by Sector (Telecoms, healthcare, financial services, and education)
   7. Regulated Access Rights/Duties by Jurisdiction (ex. EU)

B. Resource Subject/Owner Variations
    1. Natural Person
    2. Legal Person (Corporation or Government)
    3. Legal Representatives of Natural or Legal Persons

C. Resource Server Variations
    1. Things/Devices/Smart Meters
    2. Mobile Phones
    3. Product Cloud Applications
    4. Enterprise or Business Systems
    5. Government Systems

D. Requesting Party Variations
    1. Natural Person
    2. Legal Person (Corporation or Government)
    3. Legal Representatives

E. Authorization Permissions/Purposes
    1. Access
    2. Use of Identity Attributes for Authentication
    3. Use for Healthcare Monitoring /Treatment
    4. Use for Device Performance Assessment
    5. Device and Data Usage Patterns – Third Party Marketing
    6. Downstream Users and Uses

III. UMA Use Cases by Networked-Access Environment

A. Globe-Trotting Consumer/Patient with Smart, Connected Health Products

Alice, a diabetic, uses a smart Medtronic MiniMed blood glucose meter and insulin pump system and also uses a fitness wearable, the Ralph Lauren PoloTech Shirt, to manage her health. Alice uses a generic data sharing manager (AS) offered by her alma mater, Unseen University, to manage health data flow. She lives in Massachusetts but frequently travels on business to the United Kingdom, and once sought emergency treatment in London due to fainting from a low-blood-sugar condition. In the course of that treatment episode*, she allows data sharing from her home physician's portal (RS) to the UK institution (Client) and vice versa (UK institution as RS and home institution as client). Alice is the RO for the RS's and her doctors are RqPs who between them use a variety of clients. Some of her devices, or rather, the cloud services associated with them, both generate (RS) and consume (as a Client) data. When traveling, Alice also gives her cardiologist's office temporary access to her personal calendar to make it easier to schedule a series of checkup appointments upon her return.

*Simplifying assumption: Payment for the treatment is approved in some fashion, based on sufficient data being shared in appropriate directions to establish the case.

Salient Factors

- A.1.
- A.3.
- A.6.
- A.7.
- B.1.
- C.1.
- C.3.
- D.1.
- D.3.
- E.3.
- E.6.

B. Consumer-Facing Smart Meters

Alice (an RO) has digitized her entire home temperature-control process by installing a Nest digital thermostat and smoke detector (these devices are connected to a cloud service that serves as an RS). At the time of purchase and onboarding to the service, she accepted an invitation from Nest to share data for marketing purposes. In addition, Alice has permitted her local utility company* (RS) to install a smart meter for water usage in her home. She also has set up her home computer, printer, and mobile phone as part of a Home Area Network. She lives in a California community that has drought-mandated restrictions on lawn watering. She has recently received a fine in the mail for exceeding her water usage limit.** In the last month, based on having bought products from these companies recently, she has also been receiving telephone and mail solicitations for Whirlpool laundry systems (RqP) as well as Jawbone wearable technology (RqP), the products of each of which can easily integrate with the Nest platform. She takes advantage of one of the offers.

*Who "owns" the data about water usage? Resource owner just means "has the right to control access". The utility company may think they're the RO, but putting UMA in place presumes they've deferred control to the homeowner.

**She can't prevent the state government from knowing how much water she used. In fact, the utility is the govt, and can share with other agencies. There are other bases for data access than consent, and it's inappropriate to offer consent options to someone who might refuse, when access might still be given. See 2017-03-03 notes.

Salient Factors

- A.1.
- A.3.
- A.5.
- B.1.
- C.1.
- C.5.
- D.2
- E.1.
- E.4.
- E.5.
- E.6.

C. Consumer-Facing Mobile Phone Applications

Verizon (RS, and either an enterprise RO or applying enterprise IAM technology and techniques falling under its Ts & Cs to throttle Alice's access appropriately) would like to leverage the identity attribute data collected in-person at its large network of stores to become an identity provider. However, Verizon is required (not any longer!) by federal law to obtain the account-holder's consent before giving access or sharing the identity attributes for the purpose of identity transactions. To obtain the consumer consents for this purpose, Verizon uses a third-party intermediary, Erikson (AS), which is contractually bound to the GSMA Mobile Connect Standard (so the AS is functioning as an OpenID Provider). At the same time, Erikson serves as a broker of online identity attributes for CITI (RqP) in completing commercial transactions. Though living in the United States, Alice (RO) routinely conducts online commercial transactions with entities in China and the United Kingdom. When an RqP needs to authenticate Alice in an online transaction*, the RqP requests the AS to confirm or verify selected identity attribute information that has been collected by Verizon, her mobile phone account provider. The AS has contractual arrangements with Alice, the RS, and the RqP that enable the AS to broker the consents and confirm Alice's digital identity attributes for authentication purposes. The AS then reports the fact of a confirmation to the RqP. In compliance with federal law, the AS also informs Alice about each authentication request and retains a log of all such requests.

*We are assuming an "Alice-to-Alice" (SSO-like) sharing situation here, such that Alice is available at run time to consent, and actually authenticate freshly as well.

Salient Factors

- A.2.
- A.3.
- A.6.
- B.1.

- C.2.
- C.3.
- C.4.
- D.2.
- D.3.
- E.2

D. Consumer-Facing Financial Online/Cloud Applications

Alice wants to share access to her official last-year's income forms (T-4 forms, as she's Canadian) with her chartered accountant Bob. Alice is the RO and Bob is the RqP. Her paycheck applications, run by SimplePay and Wave Accounting, are RS's that expose an API and scopes for accessing her income data, such as `read`. Bob uses a tax return preparation Client app called Parsley. She has only hired him through the end of this year, and wants to cut off sharing this data at the end of this period. A central data-sharing hub application (AS) helps her manage her data exposure to Bob and others from one place.

Salient Factors

- A.3.
- A.6.
- B.1.
- B.3.
- C.3.
- C.4.
- C.5.
- D.1.
- D.3.
- E.1.
- E.6.

E. Guardian of Underage Child

Alice has a minor nephew (called a Resource Subject for now) who is in the child dependency system and for whom she has been appointed a guardian. She is able to access confidential records relating to her nephew and authorize sharing of his medical records using the AS platform. All of the access and sharing policies offered by the AS strictly follow the evolving information privacy and security requirements of California state law and Santa Clara regulations.

Salient Factors *(double-check to see if all are still relevant after deleting some details*)

- A.4.

- B.1
- B.2.
- B.3.
- C.5.
- D.2.
- D.3.
- E.1.
- E.3.
- E.6.

F. Citizen-Facing Government Services (not reviewed yet)

Alice would like for the Virginia DMV (RO and RS) to share her identity attributes with an identity brokering service offered by Signicat (AS) for purposes of completing banking transactions as well as participating in the Health Information Exchange (HIE). When a hospital system or other RqP needs Alice to share identity attributes to prove who she is, the RqP requests the AS to confirm or verify selected identity attribute information that has been collected by the Virginia DMV. The AS has a contractual arrangement with the DMV that enables the AS to present Alice's digital identity attributes to the DMV for yes/no confirmation. The AS then reports the fact of a confirmation to the RqP. In compliance with Virginia law, the AS also informs Alice about the authentication request and retains a record of all such requests.

Salient Factors

- A.3.
- A.5.
- A.6.
- B.1.
- B.3.
- C.3.
- C.5.
- D.2.
- D.3.
- E.2.

IV. Implications for Creating a UMA Legal Framework

A. Mapping UMA Roles, Obligations and Liabilities to Information Privacy, Information Security, Federated IdM, and eID Frameworks

1. Resource Subject
2. Resource Owner/Access Rights Holder
3. Resource Server
4. Authorization Server

5. Requesting Party
6. Relying Parties (Out of UMA Network)

B. Intermediary Service Provider Liability Issues
    1. Unauthorized Access, Use or Dissemination of Protected Data (by AS)
    2. Mistaken Identification of Requesting Parties (by AS)
    3. Failure to Enforce Access Policies with Third Party Providers (by AS)
    4. Failure to Enforce Access Policies with Requesting Parties (by AS)
    5. Unauthorized Dissemination of Identity Attributes (by Identity Brokers)

C. Strategies for Limiting Liability
    1. Contractual
    2. Insurance
    3. Compliance with Jurisdiction-Specific Laws
    4. Compliance with Data/Industry-Specific Regulations

Parking Lot:

- Create diagrams and/or demos and/or screenshots that illustrate the use cases?
- Find jurisdictionally parallel use cases for the ones above?