The Emerging Legal Framework for Identity and Access Management

Thomas J. Smedinghoff  
Edwards Wildman Palmer LLP  
Chair: ABA Identity Management Legal Task Force  
May 9, 2012
ABA Legal Task Force
Overview
American Bar Association
Identity Management Legal Task Force - 1

♦ It’s an open project:
  ♦ Participants include lawyers, non-lawyers, IdM technology experts, businesspersons, and other interested persons
  ♦ From businesses, associations, universities, and government agencies
  ♦ From U.S., Canada, EU, Australia, etc.

♦ ABA Task Force Website (and sign up for listserv) at –
  ♦ http://apps.americanbar.org/dch/committee.cfm?com=CL320041
American Bar Association
Identity Management Legal Task Force - 2

♦ **Goals**
  ♦ Identify and analyze the *legal issues* that arise in connection with the development, implementation and use of federated identity management systems;
  ♦ Identify and evaluate models for an appropriate *legal framework*;
  ♦ Develop *sample terms and contracts* that can be used by parties

♦ **Draft Report** (three parts)
  ♦ IdM fundamentals and terminology
  ♦ Legal regulation of, and barriers to, identity management
  ♦ Structuring a legal framework for an identity system

Draft Report available at –
http://apps.americanbar.org/dch/committee.cfm?com=CL320041
Identity Management Basics
Two Key Questions We’re Trying to Address For Online Transactions

♦ “Who are you?” (Identification)
  ♦ Assigning attributes to individuals (or companies, or devices)
    ♦ Name, address, age, status (e.g., student or faculty), company, authority, credit rating, gender, model number, serial number, etc.
    ♦ A one-time (offline or online) process called “identity proofing”
  ♦ Issuing a credential
    ♦ Drivers license, passport, ATM card, UserID, digital certificate, smart card, etc.
  ♦ Typically a one-time event

♦ “How can you prove it?” (Authentication)
  ♦ Verifying that the person online is the person previously identified
  ♦ Correlate a person to a credential (drivers license, UserID, etc.) via an authenticator (e.g., picture, password, etc.)
Three Key “Roles”

- **Subject** (a/k/a user, principal, or customer)
  - The person (entity, or device) that is identified
  - The subject of assertions/claims about his/her identity

- **Identity Provider** (a/k/a credential service provider, CA)
  - Responsible for **identity proofing** of Subject and issuing a Credential
  - Producer of assertions/claims about a Subject’s identity to a Relying Party via a Credential

- **Relying Party** (a/k/a service provider, vendor)
  - Consumer of identity assertions/claims
  - Relies on assertion to make authorization decision
The Basics of an Identity Transaction

1. A **Relying Party** wants to know “something” about the identity of a **Subject**, such as –
   - basic identifying information (e.g., name, account number, etc.)
   - status or role (e.g., employment, student, membership)
   - qualifications (e.g., credit rating, authority)
   - age or nationality, etc.

2. An **Identity Provider** has previously issued a digital “**Credential**” to make an “assertion” or “claim” about the identity of the Subject (or issues one upon request)

3. The Credential is **communicated** to the Relying Party and **authenticated**

4. The Relying Party **relies** on the assertion/claim from the Identity Provider and does business with the Subject
Traditional Two-Party Approach

Data Subject

Employee or Customer

(User ID and Password)

Identity Provider & Relying Party

Employer or Bank
The Developing Three-Party Approach: Federated Identity Management

ATM Example

- **Identity Provider**: (Bank A)
- **Subject**
- **Relying Party**: (ATM Card) (Bank B)
- **Relying Party**: (ATM Card) (Bank C)
- **Relying Party**: (Verification) (Bank D)
U.S. National Strategy For Trusted Identities in Cyberspace (NSTIC)

 Issued by White House on April 15, 2011: www.nist.gov/nstic

 Vision: Identity systems that --
 - Are “secure, efficient, easy to-use, and interoperable”
 - Promote “confidence, privacy, choice, and innovation”

 Key NSTIC goals
 - Develop a comprehensive Identity Ecosystem Framework
   - “the overarching set of interoperability standards, risk models, privacy and liability policies, requirements, and accountability mechanisms that govern the Identity Ecosystem”
 - Private sector to lead the effort to build & implement
 - Federal government to provide support
Building the Legal Framework
All Online Identity Systems Require Rules

♦ **Business & Technical Rules**
  ♦ **Content**
    ♦ Business and Technical specifications, process standards, policies, operational procedures, performance rules and requirements, assessment criteria, etc.
  ♦ **Purpose**
    ♦ Make it work – from a functional perspective
    ♦ Make it trustworthy – willingness to participate

♦ **Legal Rules (Contractual)**
  ♦ **Content**
    ♦ Contractual obligations, including agreement to follow Business & Technical Rules
  ♦ **Purpose**
    ♦ Define and govern the legal rights and responsibilities of the participants
    ♦ Address liability and risk allocation
    ♦ Provide mechanism for enforcement of rights / Address dispute resolution
    ♦ Make it trustworthy – willingness to participate
Those Rules Go By Various Names

- **Trust Framework** – NSTIC / Kantara / OIX
- **Operating Policies** - SAFE-BioPharma
- **Federation Operating Policies and Practices** - InCommon
- **Operating Rules** – FIXs / CAHQ (health info exchange)
- **Operating Rules and System Documentation** - IdenTrust
- **Common Operating Rules** - CertiPath
- **Guidelines** – CA/Browser Forum
- **Operating Regulations** - Visa (credit)
- **Operating Rules** – NACHA (electronic payments)
- **Operating Procedures** – Bolero (e-bills of lading)
1. Business & Technical Rules: (Components Necessary to “Make it Work”)

- Technical Specifications
- Identity Proofing
- Privacy Standards
- Security Standards
- Audit & Assessment Oversight
- Credential Management
- Credential Issuance
- Authentication Requirements
- Reliance Rules
- Enrolment Rules

**Partial listing of Business & Technical Rules**

**NOTE:** Must comply with any existing law; Also may be supplemented by existing law.
2. Legal Rules  
(To Govern Legal Rights of the Parties)

Partial listing of Legal Rules

- Liability for Losses
- Warranties
- Dispute Resolution
- Measure of Damages
- Enforcement Mechanisms
- Termination Rights

Existing Law as Supplemented and/or Modified by Private Legal Rules
Putting It All Together to Form Enforceable “Operating Rules”

Business and Technical Rules

- Technical Specifications
- Credential Issuance
- Authentication Requirements
- Reliance Rules
- Credential Management
- Identity Proofing
- Privacy Standards
- Security Standards
- Audit & Assessment Oversight
- Enrolment Rules

Enforcement Element

Contract(s): “I Agree” to . . .

Legal Rules (Contractual)

- Liability for Losses
- Warranties
- Termination Rights
- Dispute Resolution
- Measure of Damages
- Enforcement Mechanisms
- Auditing & Assessment Oversight
- Oversight
- Credentialed Management
- Security Standards
- Identity Proofing
- Enrolment Rules
- Privacy Standards
- Audit & Assessment Oversight
- Technical Specifications
- Credential Issuance
- Authentication Requirements
- Reliance Rules
- Credential Management
Operating Rules Are Governed By Existing Laws

**Laws & Regulations** (in all relevant jurisdictions)
- Authentication law
- Data retention law
- Privacy law
- IdM laws
- Tort law
- EU Data Protection Directive
- Crypto regulations
- PKI laws
- EU E-Signatures Directive
- Contract law

**Business & Technical Rules**
- Technical Specifications
- Credential Issuance
- Authentication Requirements
- Reliance Rules
- Credential Management
- Identity Proofing
- Privacy Standards
- Security Standards
- Audit & Assessment Oversight
- Business Processes

**Legal Rules (contractual)**
- Contract: “I Agree” to . . .
- Liability for Losses
- Warranties
- Termination Rights
- Dispute Resolution
- Enforcement Mechanisms
- Measure of Damages

* Written by governments; applies to all identity systems
** Written by private parties; a/k/a “trust framework;” applies to a specific identity system
All Identity Systems Use **Private** Operating Rules that Operate Within a **Public** Legal System

* Written by governments; applies to all identity systems
** Written by private parties; a/k/a “trust framework;” applies to a specific identity system
Key Legal Issues - Privacy

♦ Must comply with existing privacy law
  ♦ In all relevant jurisdictions
  ♦ And such laws may be inconsistent

♦ Can add additional privacy requirements
  ♦ To enhance trust of individual subjects
  ♦ But increases cost for other participants

♦ NSTIC views protecting privacy as key issue to incentivize participation by Subjects
  ♦ Proposes that identity systems be based on -
    ♦ Fair Information Practice Principles
    ♦ A “user-centric” approach to data protection
  ♦ Privacy will be major focus of NSTIC Ecosystem Framework
Key Legal Issues - Liability

♦ Major concern for all participants – e.g., what is . . .
  ♦ Subject liability for failing to protect password or key?
  ♦ Identity Provider liability for incorrect identification?
  ♦ Relying Party liability for relying on false identity information?

♦ Existing public law is often ambiguous or unacceptable

♦ Solution is to allocate liability by contract, to the extent possible – i.e., to make up the liability rules
  ♦ Consider credit card system example
  ♦ Requires binding everyone to the contract

♦ BUT NOTE: Liability is a zero-sum game

♦ NSTIC recognizes liability is a primary barrier
  ♦ Proposes contractual allocation; recognizes legislation may be needed
Many Ways to Write the Liability Rules

- Warranty model – focus on stated or implied guarantees
- Tort model – focus on standards of conduct; negligence
- DMV model – no IdP liability; other roles bear all risk
- Credit card model – no Subject liability; others bear risk
- Contractual model – negotiated risk allocation
- Strict liability – regardless of fault
- Liability caps model
- Restrictions on ability of IdP to limit its liability

But recognize that if you don’t write them --
- You are subject to the uncertainties of existing law
- In multiple jurisdictions
Other Common Legal Problems For Contract-Based Operating Rules

♦ The enforceability problem
  ♦ How to bind all participants in an enforceable contractual framework?
  ♦ What about non-participants?

♦ The uncertainty problem
  ♦ Lack of clarity re the rules under existing law

♦ The cross-border problem
  ♦ Addressing the problem of differing legal regimes

♦ The non-waivable statute problem
  ♦ Some laws regulate Identity management systems
  ♦ Can’t be changed by contract (e.g., consumer)
Building the Legal Framework Under NSTIC
Start with Layer 1 – Existing Laws and Regulations

<table>
<thead>
<tr>
<th>Laws &amp; Regulations* (in all relevant jurisdictions)</th>
<th>Data security law</th>
<th>E-transaction law</th>
<th>Breach Notification law</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication law</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data retention law</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy law</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IdM law</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tort law</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EU Data Protection Directive</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Crypto regulations</td>
<td>PKI laws</td>
<td>EU E-Signatures Directive</td>
<td>Contract law</td>
</tr>
<tr>
<td>Law of negligent misrepresentation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rules of evidence</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consumer protection law</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warranty law</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Written by governments; applies to all identity systems
Add Layer 2 -- the NSTIC Concept of a Voluntary Identity Ecosystem Framework

Identity Ecosystem Framework – NSTIC***
(The overarching set of interoperability standards, risk models, privacy and liability policies, requirements, and accountability mechanisms that structure the Identity Ecosystem)
- To be written by NSTIC Steering Group
- Not Law (but must comply with law)
- Voluntarily adopted by identity systems
- Adherence accredited - Trustmark

* Written by governments; applies to all identity systems; compliance is mandatory
*** Written by NSTIC Steering Group; compliance is voluntary
Add Layer 3 – Individual System Operating Rules
(May or May Not Conform to NSTIC Ecosystem Framework)

Laws & Regulations*
(in all relevant jurisdictions)

- Data security law
- E-transaction law
- Breach Notification law

Identity System K Operating Rules**
- Consumer protection law
- Warranty law

Identity System 4 Operating Rules**
- Rules of evidence

Identity System X Operating Rules**
- Law of negligent misrepresentation

Identity System Y Operating Rules**

Identity System D Operating Rules**

Identity System 99 Operating Rules**

* Written by governments; applies to all identity systems
** Written by private parties; a/k/a “trust framework;” applies to a specific identity system
The Overall Goals

♦ Develop acceptable operating rules that –
  ♦ Provide enforceable rules for a workable and trustworthy identity system that are binding on all participants
  ♦ Adequately protect the rights of all parties
  ♦ Fairly allocate risk and responsibilities among the parties
  ♦ Provide legal certainty and predictability to the participants
  ♦ Comply with / work in conjunction with existing law
  ♦ Works cross-border (state or country)
Further Information

Thomas J. Smedinghoff
Edwards Wildman Palmer LLP
225 West Wacker Drive
Chicago, Illinois 60606
312-201-2021
TSmedinghoff@edwardswildman.com

American Bar Association
Identity Management Legal Task Force
http://apps.americanbar.org/dch/committee.cfm?com=CL320041
Shibboleth Workshop Series
http://www.incommon.org/educate/shibboleth/

July 16-17 – Baltimore, Maryland - UMBC
Evaluation
Please complete the evaluation of today’s IAM Online:

IAM Online Announcement List
Email sympa@incommon.org with the subject: subscribe iamonline

Thank you to InCommon Affiliates for helping to make IAM Online possible.