Identity Management
Legal Task Force

Overview
Background

♦ Similar to prior ABA emerging technology law projects
  ♦ EDI “Model Trading Partner Agreement” project in the late 1980s
  ♦ PKI “Digital Signature Guidelines” project in early 1990s

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

♦ ABA Task Force Website (and sign up for listserv) at –
Goals and Collaboration

♦ Goals
  ♦ Identify and analyze IdM legal issues
  ♦ Identify and propose appropriate legal solutions for federated systems
  ♦ Identify and evaluate models for an appropriate legal framework

♦ Working with many groups, including –
  ♦ Open Identity Exchange (OIX)
  ♦ U.S. NSTIC / IDESG
  ♦ Kantara Initiative
  ♦ Internet Society
  ♦ Standards groups, including ITU-T, ISO, ANSI / NASPO
  ♦ UN Commission on International trade Law (UNCITRAL)
Projects Include . . .

♦ Comprehensive Legal Report

♦ Three parts -
  ♦ What is identity management, and how does it work?
  ♦ What are the legal issues of IdM?
  ♦ How can we address those issues and structure the legal framework for an identity system?
Meeting
Goals and Objectives
Meeting Goals and Objectives

♦ Communication
  ♦ Compare/understand US vs. EU legal perspectives
  ♦ Begin EU-U.S. dialog regarding cross border legal solutions

♦ Substantive Legal Issues
  ♦ Identify legal issues
  ♦ Analyze and address privacy issues
  ♦ Analyze and address liability issues
  ♦ Consider cross-border legal issues and challenges
  ♦ Consider potential legal solutions
  ♦ Consider desirability and possible content of international legal rules
Topics Covered

♦ Today
  ♦ Identity legal environment and legal issues
  ♦ Compare US and EU legal views – at a policy level
  ♦ Compare legal approaches adopted by current projects
  ♦ Privacy issue
  ♦ Reception

♦ Tomorrow
  ♦ Liability issue
  ♦ Cross-border challenges
  ♦ Possible legal solutions
  ♦ Possible international rules
  ♦ Next steps
Topics **NOT** Covered

- SAML
- ISO/IEC 29115
- ISO/IEC PRF 29191
- ITU x.1252
- NIST 800-63 M-04-04
- ISO 27001
- PKI
- x.509
- LOA
- ID proofing standards
- encryption standards
- ID proofing standards
- principles, commandments, codes, guidelines
- best practices
The Three-Level IdM Legal Environment
All Online Identity Systems Require Privately Developed, System-Specific, Rules

♦ **Purpose**
  ♦ Make it work – from a functional perspective
  ♦ Make it trustworthy – willingness to participate
  ♦ Define & govern the legal rights and responsibilities of the participants

♦ **Content of rules**
  ♦ Technical specifications
  ♦ Business processes and standards
  ♦ System policies and operational procedures
  ♦ Role performance obligations and requirements
  ♦ Assessment criteria
  ♦ Private legal rules – e.g., warranty, liability, dispute resolution
  ♦ Etc.
  ♦ Agreement to follow / be bound by the foregoing rules
Those Private Rules Go By Various Names

- **Trust Framework** – NSTIC / Kantara / OIX
- **Scheme Rules** – UK IDAP
- **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)
Business & Technical Rules: (Components Necessary to “Make it Work”)

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

Existing Law

Partial listing of Business & Technical Rules

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

Existing Law as Supplemented and/or Modified by Private Legal Rules

Partial listing of Legal Rules

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

Existing Law

Enforcement Element

Contract(s): “I Agree” to . . .

Legal Rules (Contractual)

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

Existing Law
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

**Operating Rules**

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

**Business & Technical Rules**

**Contract:**
"I Agree" to...

**Legal Rules (contractual)**

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

- Consumer protection law
- Warranty law
- Law of negligent misrepresentation
- Rules of evidence
- Crypto regulations
- PKI laws
- EU E-Signatures Directive
- Contract law

* Written by governments; applies to all identity systems

** Written by private parties; applies to a specific identity system
Identity Systems Use Private Operating Rules that Operate Within the Public Legal System

### Laws & Regulations*

* (in all relevant jurisdictions)

- Data security law
- E-transaction law
- Breach notification law
- Consumer protection law
- Warranty law
- Rules of evidence
- Law of negligent misrepresentation

**Identity System X Operating Rules**

**Identity System Y Operating Rules**

**Identity System Z Operating Rules**

**Certipath Operating Rules**

**SAFE-BioPharma Operating Rules**

**Facebook Connect Operating Rules**

**InCommon Operating Rules**

---

* Written by governments; applies to all identity systems

** Written by private parties; applies to a specific identity system
Three Levels of Law/Rules Governing ID Systems

- **Level 1** - Existing law, regulations, and common law
  - Public law
  - Enacted and enforced at the country level
  - Typically not specific to identity – e.g., negligence law, contract law
  - Not always clear how applies to identity

- **Level 2** - Identity-specific law or voluntary frameworks
  - Public or private law
  - E.g., NSTIC – IDESG Identity ecosystem framework
  - E.g., EU E-Signatures Directive, eID Regulation

- **Level 3** - Individual identity system operating rules
  - Private law – typically contract-based
  - Developed specifically for a particular identity system
The Identity Legal Framework --
Start with Level 1 – Existing Country Laws and Regulations

**Laws & Regulations***
(in all relevant jurisdictions)

- Data security law
- E-transaction law
- Breach Notification law
- Consumer protection law
- Warranty law
- Rules of evidence
- Law of negligent misrepresentation
- PKI laws
- EU E-Signatures Directive
- Contract law
- EU Data Protection Directive
- Crypto regulations
- PKI laws
- EU E-Signatures Directive
- Crypto regulations
- IdM law
- Tort law
- Privacy law
- Data retention law
- Authentication law

* Written by governments; applies to all identity systems

We need to identify existing law relevant to IdM

Note also that these laws may conflict from jurisdiction to jurisdiction
Add Level 2 – in the U.S., Voluntary ID-Specific Rules Called the Identity Ecosystem Framework

* Written by governments; applies to all identity systems
Add Level 2 – in the EU, Mandatory (?) ID-Specific Rules Called the eID Regulation or ??

* Written by governments; applies to all identity systems
Add Level 3 – Individual Identity System Operating Rules (May or May Not Conform to Level 2 Rules)

**Laws & Regulations**
* (in all relevant jurisdictions)

- Data security law
- E-transaction law
- Operating Rules / Identity System K**
- Consumer protection law
- Warranty law
- Operating Rules / Identity System D**
- Operating Rules / Identity System 4**
- Rules of evidence
- Operating Rules / Identity System X**
- Operating Rules / Identity System Z**
- EU E-Signatures Directive
- Contract law
- EU Data Protection Directive
- PKI laws
- EU E-Signatures Directive
- Authentication law
- Crypto regulations
- PKI laws
- EU E-Signatures Directive
- Operating Rules / Identity System 99**
- Operating Rules / Identity System X**
- Operating Rules / Identity System Z**

**EU eID Framework**

**U.S. NSTIC ID Ecosystem Framework**

* Written by **governments**; applies to **all** identity systems

** Written by **private parties**; applies to a **specific** identity system
Challenges Include . . .

♦ How do we reconcile jurisdictional differences at Level 1?

♦ How do we reconcile jurisdictional differences at Level 2?

♦ Do We Need “Level 0” Rules? -- I.e., International Rules?
  ♦ To address conflicts in Level 1 general country laws?
  ♦ To address conflicts in Level 2 identity-specific country laws?
Identifying the Legal Issues
### What Level 1 Laws Affect Identity Systems?

#### Laws & Regulations*

*(in all relevant jurisdictions)*

<table>
<thead>
<tr>
<th>Authentication law</th>
<th>Data security law</th>
<th>E-transaction law</th>
<th>Breach Notification law</th>
</tr>
</thead>
<tbody>
<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></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

* Written by governments; applies to all identity systems
Law Governing Collection, Use, and Transfer of Identity Data

- Privacy / data protection law
- Law governing reuse of public data
  - E.g., EU Directive on reuse of public sector information 2003/98/EC
- Law governing reuse of government-issued identity numbers
  - E.g., U.S. laws regulating use of SSN
  - E.g., EU country laws regulating reuse of national identification numbers
- Law governing enrollment by individual subjects
  - Identity fraud / identity theft laws
  - False statement acts (made to government)
Law Governing Identity Credentials

♦ Law governing use of identifiers
  ♦ E.g., Article 29 Working Party objections to Microsoft .net passport unique identifier

♦ Law governing issuance of identity credentials
  ♦ E.g., EU e-signatures directive requirements for qualified certificates
  ♦ E.g., EU e-signatures directive requirements for certification-service-providers issuing qualified certificates

♦ Law governing use of identity credentials
  ♦ E.g., EU e-signatures directive rules re CSP limits on use of qualified certificates
  ♦ E.g., Washington state PKI law re certificate reliance limits

♦ Law governing cross recognition of identity credentials
  ♦ E.g., EU e-signatures directive rules for cross recognition of qualified certificates
Law Governing the **Accuracy** of Identity Information

- Warranty law
- Tort of negligent misrepresentation
- Defamation
- Privacy law
  - Accuracy
  - Access and correction rights
- Other
  - E.g., U.S., Fair Credit Reporting Act
  - E.g., EU e-signatures directive requirements
Law Governing the Availability of Identity Information

- Privacy law
  - E.g., EU Data Protection Directive right of access for data subjects
- Data retention laws
- Data destruction laws
- Business continuation / termination laws
Law Governing the **Security** of Identity Information

- **Duty to provide data security**
  - E.g., obligation impose by numerous U.S. laws
  - E.g., obligation impose by EU Data Protection Directive and country laws

- **Duty to disclose data breaches**
  - E.g., U.S. state breach notification laws (46 states)
  - E.g., proposed EU data protection regulation
Law Governing Quality of Identity Services

- Private accrediting
  - Negligent endorsement
    - E.g., liability of issuers of trustmark
    - Trademark and trustmark law
- Negligent credentialing
- Government licensing or accrediting of IdPs
  - E.g., licensing scheme under Washington State PKI law
- Qualification requirements to participate
  - E.g., EU e-signatures directive requirements for CSPs issuing qualified certificates
Law Governing Ownership of Identity Credentials

♦ Ownership of what?
  ♦ Physical container
  ♦ Data itself
  ♦ Assertion expressed or implied by the credential – the binding
  ♦ Benefit or entitlement evidenced by the credential
  ♦ Something else

♦ Tangible property rights
♦ Intangible personal property rights
General Legal Barriers

♦ Existing public law does not address all relevant issues
♦ Uncertainty / ambiguity of existing public law
♦ Existing public law may provide inappropriate rules/results
♦ Jurisdictional variations / conflicts – Cross-border issues
♦ Inability to modify some existing public laws by contract
♦ Variation in public law rules based on –
  ♦ Nature of the participant (e.g., consumer vs. business vs. government)
  ♦ Nature of the information (e.g., sensitive data)
  ♦ Nature of the use (e.g., high value vs. social media)
  ♦ Nature of the harm (e.g., economic loss vs. physical injury)
What Have We Missed?

♦ What else is there?
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