Basic Premise

• A lot is happening on the IdM legal & legislative front!!
  – “The train has left the station!”

• These developments will have a significant impact on all participants in the identity ecosystem
  – Important to monitor
  – Important to provide input

• **Goal** -- Seek your input and ideas regarding the direction that domestic and international IdM legislative efforts should take
Introductory Topics

• Current Legal Framework Governing IdM Systems
• Recent Legal Developments
• Upcoming Legal Initiatives
• Possible Approaches to New Legislation
Current Legal Framework
Governing Identity Systems Today
Rules, Rules, Rules -- It’s All About Rules

• All federated (multiparty) identity systems require business, technical, and legal rules
  – To make the system “operationally functional”
    • i.e., so that it works properly
  – To make the system “trustworthy”
    • i.e., so that people will use and rely on it
  – To make the system “legally functional”
    • i.e., so that rights and obligations are defined and enforceable

• Analogous examples –
  – Credit card systems (e.g., Visa, MasterCard, Amex, Discover)
  – Fund transfer systems (e.g., SWIFT, ACH)

• Legal rules make the business and technical rules enforceable
Where Do the Legal Rules Come From? -- Three Basic Levels of IdM Legal Rules

1. **General law** (public law)
   - Existing statutes, regulation, and case law
   - **Not designed to address identity issues, but will often apply**
   - E.g., contract law, tort law, privacy law, EU Data Protection Directive, EU-U.S. Safe Harbor (now invalid), commercial law, fraud law, family law, competition law, etc.

2. **Identity Management-specific law** (public law)
   - New statutes and/or regulations
   - **Written specifically to address online identity system issues**
   - E.g., EU eIDAS Regulation, Virginia Electronic Identity Management Act

3. **Identity System rules** (private law)
   - Often called trust frameworks, scheme rules, or operating rules
   - Often incorporate technical standards, business rules, best practices, etc.
   - Typically enforced by contract
Identity System Law:
Three Levels of Rules Can Govern

1. General Law (Existing)
   - Contract law, Tort law, Commercial law, Privacy law, Safe Harbor, Fraud law, Competition law, etc.

2. Identity Mgmt-Specific Law (NEW)
   - EU eIDAS Regulation,
   - Virginia IdM Act,
   - UNCITRAL?
   - ULC?

System Rules must comply with Levels 1 and 2 above

3. System Rules for Identity System A
   - System Rules for Identity System B
   - System Rules for Identity System N
Identity System Law: Three Levels of Rules Can Govern

1. General Law (Existing)
   - Contract law, Tort law, Commercial law, Privacy law, Safe Harbor, Fraud law, Competition law, etc.

2. Identity Mgmt-Specific Law (NEW)
   - EU eIDAS Regulation,
   - Virginia IdM Act,
   - UNCITRAL?
   - ULC?

System Rules must comply with Levels 1 and 2 above

3. System Rules for Identity System A
   - System Rules for Identity System B
   - System Rules for Identity System N

Today’s Focus
- e.g., Connect.gov; GOV.UK Verify, SAFE-BioPharma; TSCP; IdenTrust; InCommon; IDEF Baseline Functional Requirements; IdV Standards; LOA Standards
Identity System Law: 
Three Levels of Rules Can Govern

1. General Law (Existing)
   - Contract law, Tort law, 
   - Commercial law, Privacy 
   - law, Safe Harbor, Fraud 
   - law, Competition law, etc.

2. Identity System-Specific Law (NEW)
   - EU eIDAS Regulation, 
   - Virginia IdM Act, 
   - UNCITRAL? 
   - ULC?

System Rules must comply with Levels 1 and 2 above

3. System Rules for
   - Identity System A
   - Identity System B
   - Identity System N

Today’s Focus

Private Law (Rules)

Public Law (Rules)

e.g., Connect.gov; GOV.UK Verify, SAFE-BioPharma; TSCP; IdenTrust; InCommon; 
IDEF Baseline Functional Requirements; IdV Standards ; LOA Standards
Key Recent Legal Developments (at Level 2)
Level 2 – Identity System-Specific Law (1)
EU – eIDAS Regulation (July 2014)

- Adopted July 16, 2014; applies to all EU member states
- Applies to public sector only
- The Regulation addresses --
  - Levels of Assurance standards
  - Mutual recognition of identity credentials in cross-border transactions
  - Duty to notify of breach
  - IdP liability
  - Privacy
  - Interoperability framework
EU – eIDAS Regulation
– Levels of Assurance

• Defines three levels of assurance (LOA)
  – **Low** – a limited degree of confidence in the asserted identity
  – **Substantial** – a substantial degree of confidence in the identity
  – **High** – a higher degree of confidence in the asserted identity than LOA substantial

• Appears to generally correspond to NIST levels 2, 3, and 4
EU – eIDAS Regulation
-- Levels of Assurance

• September 8, 2015 Implementing Act specifies minimum technical specifications and procedures for LOAs in following areas –
  – Enrollment
    • Application and registration
    • Identity proofing and verification
  – Credential management
    • Credential characteristics and design
    • Credential issuance, delivery & activation
    • Credential suspension, revocation, and reactivation
    • Credential renewal & replacement
  – Authentication
  – Management and organization
    • Published notices and user information
    • Data security management
    • Record keeping
    • Facilities and staff
    • Technical controls
    • Compliance and audit
EU – eIDAS Regulation
– Mutual Recognition

• Applies to cross-border online public sector identity transactions

• Requires mutual recognition of identity credentials in cross border public sector transactions

• **If** a public sector body in one EU member state requires identity credentials of LOA “substantial” or “high” (3 or 4) for online access to a service provided by that public sector body -
  
  – **Then**, it **must accept** identity credentials at an equivalent or higher LOA issued in another member state under an eID scheme included on a **list published by the EU Commission**
EU – eIDAS Regulation
– Qualification for Mutual Recognition

• Member state may “notify” the Commission of an identification scheme (i.e., get on the Commission’s approved list) where –
  – Credentials are issued by the notifying state or by private sector party “recognized” by the state
  – Credentials can be used to access at least one public sector service in the notifying member state;
  – The ID scheme and credentials meet LOA requirements of the implementing act
  – The member state ensures that identifying data uniquely representing a person is attributed to that person in accordance with the implementing act (identification)
  – The party issuing the credential ensures that the credential is attributed to the person so identified in accordance with the implementing act (credential issuance)
  – The member state ensures availability of authentication online so that RPs can confirm the credential data
EU – eIDAS Regulation
– Security Breach

• If an identity scheme or authentication capability is breached or compromised member state must –
  – Notify EU Commission and other member states, and
  – Suspend or revoke authentication or compromised parts
EU – eIDAS Regulation
– Liability

• **Member state** is liable for -
  – Failure to ensure that attribute data uniquely representing a person is attributed to that person in accordance with specifications in implementing acts
  – Failure to ensure availability of online authentication

• **Party issuing credential** is liable for -
  – Failure to ensure that the credential is attributed to proper person in accordance with specifications in implementing acts

• **Party operating the authentication procedure** is liable for -
  – Failure to ensure the correct operation of the authentication procedure

• All rules cover damages to any person, whether caused intentionally or negligently
EU – eIDAS Regulation
– Privacy

• Must comply with the EU Data Protection Directive
• No other special privacy requirements
EU – eIDAS Regulation
– Interoperability Framework

• Established by Implementing Act on September 8, 2015

• Criteria -
  – Technology neutral
  – Follow EU and international standards
  – Facilitate privacy by design
  – Ensure compliance with EU Data Protection Directive

• Framework addresses –
  – Minimum technical requirements for assurance levels
  – Mapping of national assurance levels to framework
  – Minimum technical requirements for interoperability
  – Minimum requirements for set of data uniquely representing a person
  – Rules of procedure
  – Security standards
  – Dispute resolution
VA – Electronic Identity Management Act

• Enacted March 2015; Effective July 1, 2015
• Applies to public and private sector
• The Act addresses --
  – IdM standards,
  – IdP liability,
  – Trustmarks and IdP warranties, and
  – Use of credentials to comply with security requirements
VA – Electronic Identity Management Act – IdM Standards

• Establishes 7-member VA Identity Management Standards Advisory Council
  – “to advise the Secretary of Technology on the adoption of identity management standards”
  – Seven members; 2 government, plus 5 representatives of the business community

• Secretary of Technology shall approve VA Identity Management Standards in three areas –
  – Technical standards regarding verification and authentication of identity;
  – Minimum specifications that should be included in an identity trust framework; and
  – Standards concerning reliance by third parties on identity credentials
VA – Electronic Identity Management Act – Identity Provider (IdP) Liability

• IdP or identity trust framework operator **SHALL be liable** –
  – For issuance of an identity credential or trustmark that is NOT in compliance with the VA identity management standards
  – For noncompliance with any contract or identity trust framework

• IdP or identity trust framework operator **SHALL NOT be liable** –
  – For issuance of an identity credential or trustmark that IS in compliance with -
    • the VA identity management standards, and
    • any applicable contract or identity trust framework, **as long as there is no gross negligence or willful misconduct** for misuse of any identity credential by any person
VA – Electronic Identity Management Act
– Trustmarks and IdP Warranties

• Trustmark –
  – Machine-readable seal or logo
  – Provided by an identity trust framework operator to an IdP
  – To signify that IdP complies with the requirements of an identity trust framework

• Use of a trustmark is a warranty by IdP that is has complied with the rules of the identity trust framework.

• Any other implied warranties are excluded.
VA – Electronic Identity Management Act
– Comply with Security Requirements

• Use of identity credentials satisfies any requirement for a “commercially reasonable security or attribution procedure” in --
  – UCC Article 4A (governing EFT transactions)
  – UETA (governing electronic transactions)
  – UCITA (governing computer information transactions)

• Rule applies only if the credential complies with:
  – The VA identity management standards
  – The terms of any applicable contract, and
  – The applicable identity trust framework
Other – Non-Binding

IDESG – IDEF Baseline Functional Requirements

• Released October 15, 2015
• Not a law or regulation
• The Requirements provide normative rules for implementing the four NSTIC Principles –
  – Interoperability
  – Privacy
  – Security
  – Usability
• Could be voluntarily incorporated as private law (contract) at Level 3
UN/CEFACT - Transboundary Recommendation

- **UN/CEFACT** = United Nations Centre for Trade Facilitation and Electronic Business
  - Part of the United Nations Economic Commission for Europe (UNECE)
  - Serves as the focal point for trade facilitation recommendations and electronic business standards, covering both commercial and government business processes that can foster growth in international trade and related services

- Draft “Recommendation for ensuring legally significant trusted transboundary electronic interaction”

- Seeks to establish an **International Coordination Council** to provide international regulation of a **Common Trust Infrastructure** composed of nationally regulated trust services (presumably including IdM systems) to help ensure the legal significance of transboundary electronic interaction
Key Upcoming Legal Initiatives
(Why We’re Here Today)
UNCITRAL

- **UNCITRAL** = United Nations Commission on International Trade Law
- Established by the UN General Assembly in 1966
  - 60 member states elected by the UN General Assembly
  - All other member states invited to participate
- Core legal body of the United Nations system in the field of international trade law – Specializes in commercial law reform worldwide
- **Focus** – modernization and harmonization of rules on international business
- **Develops** – International Conventions (treaties); Model laws (for domestic enactment); Legislative guides; Contractual rules; and Legal guides
UNCITRAL – Project to Develop Legal Framework for IdM (1)

- **July 2015 Proposal** that UNCITRAL undertake a project to address digital identity management
- **Submitted by**
  - Austria, Belgium, France, Italy, and Poland
  - American Bar Association Identity Management Legal Task Force
- **Goal** – to provide “basic legal framework covering identity management transactions, including appropriate provisions designed to facilitate international cross-border interoperability”
- UNCITRAL agreed that the project could move forward
UNCITRAL – Project to Develop Legal Framework for IdM (2)

- Proposal identified possible topics to address, including:
  - Legal barriers
  - Trustworthiness
  - Data security
  - Liability allocation
  - Legal effect of identity authentication
  - Cross border issues
- Potential colloquium in Spring 2016
- Formal start probably Fall 2016
The Uniform Law Commission (ULC) is a non-profit unincorporated association, comprised of state commissions on uniform laws from each of the 50 states, plus DC, PR, and VI.

Established in 1892, the ULC provides U.S. states with non-partisan, well-drafted uniform legislation that brings clarity and stability to critical areas of state statutory law.

Best known for development of --

- Uniform Commercial Code (UCC), now adopted in all 50 states
- Uniform Electronic Transactions Act (UETA), now adopted in 47 states

Drafting committee meetings open to the public
Uniform Law Commission – Project to Develop U.S. Domestic Law Governing IdM

• Proposal for a Study Committee for a Uniform Act on Identity Management in Electronic Commerce
  – Submitted Summer 2015

• Appointment of a Study Committee is the first step toward establishing a committee to draft a Uniform Act on Identity Management for adoption by the 50 U.S. States

• Currently under consideration
  – Decision expected in early 2016
The Challenge Going Forward: Possible Approaches to New Legislation
What Is the Goal?

Potential IdM Legislative Goals Include . . .

- Encourage and incentivize deployment of identity systems
- Facilitate both commercial and government use of credentials
- Fix problems with existing law
  - Particularly issues that private system rules cannot resolve
- Promote trust in identity systems
- Facilitate legal recognition of identity and authentication
- Facilitate identity system and credential interoperability
- Harmonize international legal approaches
- Regulate identity systems
- Enforce use of uniform standards
- Etc.
Some Potential Principles for Identity-Specific Law

• Technology neutrality
  – No technology-specific requirements
  – Parties use any available approach to achieve requirements

• Identity system neutrality
  – Accommodate many different identity systems models
  – Recognize that there is no one-size-fits-all approach

• Adaptability
  – Accommodate future changes in technology, standards, and business models

• Party autonomy
  – Allow variation by contract
  – e.g., system rules, trust frameworks, etc.
Possible Issues That Identity-Specific Law Might Address

• Legal barriers, ambiguities, and uncertainties in existing public law
  – Liability
  – Reliance
  – Third party rights
  – Privacy of personal data
  – Legal effect of authenticated identity
  – Transfer of personal information

• Trustworthiness
  – Levels of assurance
  – Data security
  – Certification, audits, etc.
  – Presumptions

• Interoperability of identity credentials
  – Cross-system
  – Cross-border (legal interoperability)
IdM Legislation - Threat or Opportunity?

• Will it enable and facilitate – or inhibit – development of a sustainable and interoperable identity ecosystem?
• How will it affect marketplace development by the private sector?
• Do we need to encourage experimentation and innovation, or regulate to ensure uniformity and curb abuses?
• How far should Level 2 identity-specific law go?
  – What issues should it address?
  – Which issues should be left to the parties to contractually define in Level 3 System Rules?
  – How prescriptive should it be?
Closing Thoughts

• Pay attention to what is happening
• Participate in the process; provide input
• It will affect your organization
Questions?

Thomas J. Smedinghoff
Locke Lord LLP
111 S. Wacker Drive
Chicago, IL 60606
Tom.Smedinghoff@lockelord.com