2nd International Identity Management Law and Policy Meeting

May 18, 2017

OPEN IDENTITY EXCHANGE

AMERICAN BAR ASSOCIATION

Identity Management Legal Task Force

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

Where Are We?

- The technology works, but . . .
- A lot is happening on the IdM legal & policy front!!
  - "The train has left the station!"
  - But which way is it going?
- Legal and policy developments will have a significant impact on all participants in the identity ecosystem
  - Important to monitor
  - Important to provide input
- Goal – Recommendations for the direction that domestic and international IdM legislative and policy efforts should take

Introductory Topics

- Current Legal Framework for Identity Systems
- Key Recent Legal Developments – Level 2
- Key Recent Legal Developments – Level 3

Current Legal Framework Governing Identity Systems Today

Rules, Rules, Rules -- It's All About Rules

- We need system-specific rules -- All multiparty identity systems **require enforceable business, technical, operational, 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

- We are subject to general rules -- All multiparty identity systems **are subject to general laws, regulations, and court-made legal rules**
  - For better or worse!

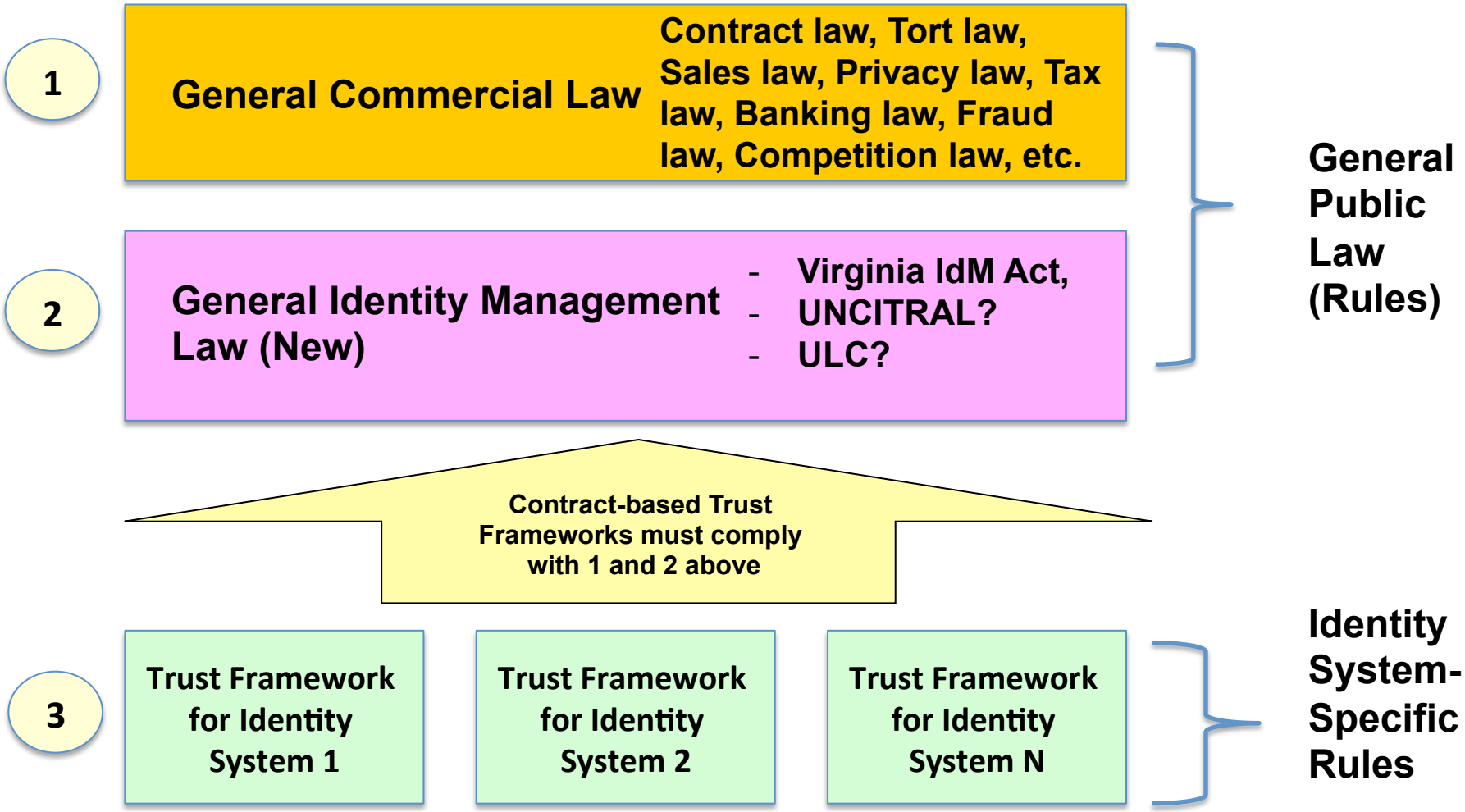
Impact of Those Rules Can Vary

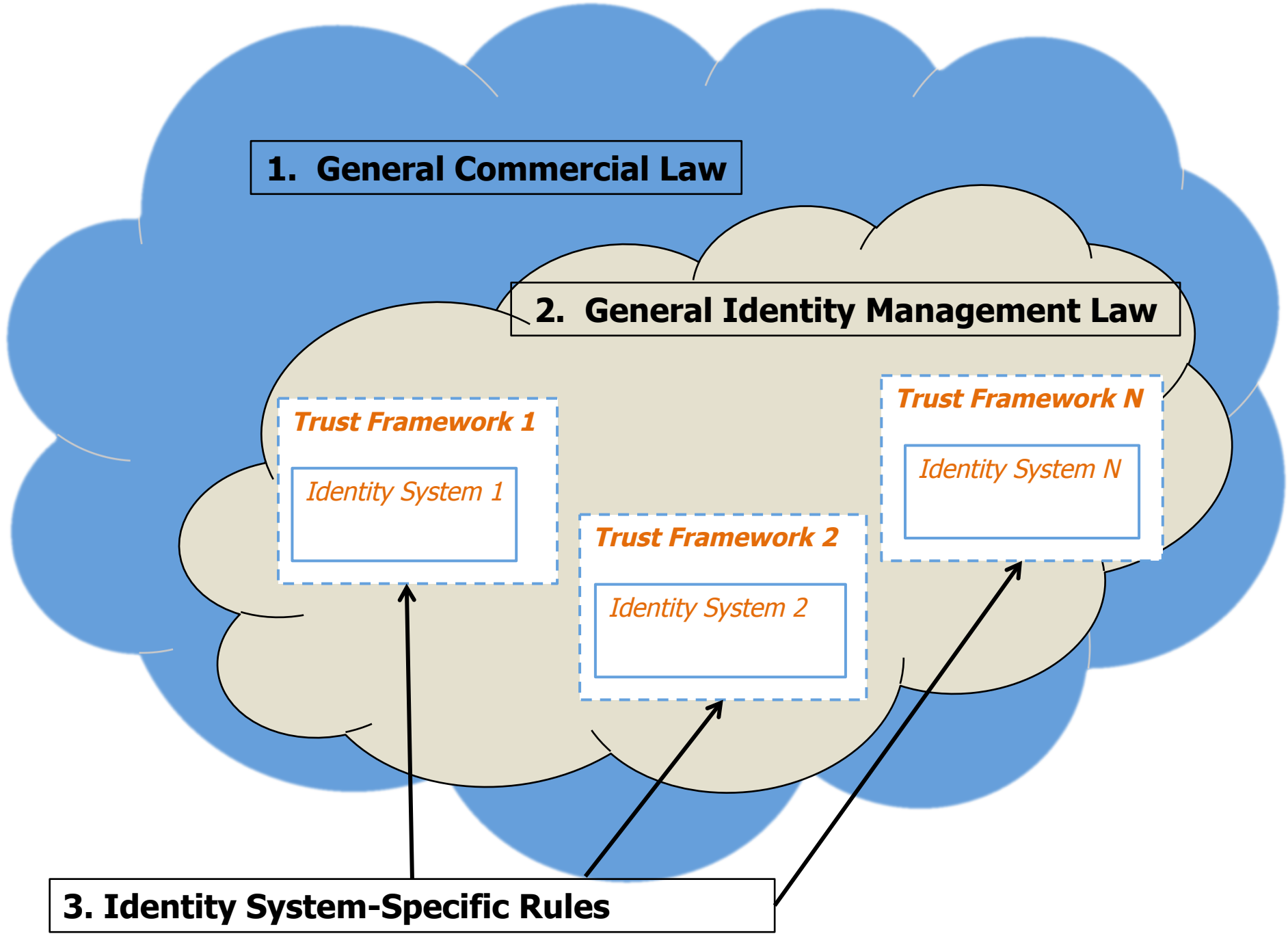
- Whether you're a provider or consumer of identity services, the rules that apply to you –
  - Can help
    - They can remove barriers to identity services
    - They can enable or facilitate or encourage identity services
    - Solve problems / protect you
    - Answer unanswered questions – e.g., what's my liability?
    - Provide needed legal certainty
  - Can hurt
    - May be vague and uncertain
    - May not address issues that need addressing
    - May provide the wrong result
    - May involve trying to fit the square peg of identity services into the round hole of existing law written for a different purpose

Where Do the Rules Come From? -- Three Basic Levels of IdM Legal Rules

1. General **Commercial** 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, Banking law, sales law, fraud law, tax law, competition law, etc.
2. General **Identity Management** law
   - New statutes and/or regulations
   - **Written specifically to address issues applicable to all identity systems**
   - E.g., Virginia Electronic Identity Management Act
3. Identity **System-Specific Rules**
   - **Often called trust frameworks, scheme rules, or operating rules**
   - **Written for a single identity system**
   - Often incorporate technical standards, business rules, best practices, etc.
   - Typically enforced by contract (may be law/regulation in public systems)

Identity System Law: Three Levels of Rules Can Govern




1. General Commercial Law
2. General Identity Management Law
Trust Framework 1
Identity System 1
Trust Framework 2
Identity System 2
Trust Framework N
Identity System N
3. Identity System-Specific Rules

Level of Law Determines . . .

- Who writes the rules
  - Level 1 and 2 = government
  - Level 3 = system operator (govt. or private party)
- Whether they apply to one identity system or all of them
  - Level 1 and 2 = apply to *all* identity systems
  - Level 3 = apply to *only one* identity system
- Granularity / specificity of rules
  - Level 1 = most general (and vague)
  - Level 3 = most detailed and system-specific
- Whether the rules can be preempted by higher law
  - E.g., statutes trump contracts

Key Recent Legal Developments

(at Level 2 – General IdM Law)

Existing Level 2 – General Identity Management Law

VA – Electronic Identity Management Act

- Enacted March 2015; Effective July 1, 2015
- Applies to all public and private sector systems
- 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

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 – IdM Project
Discussions at April 24-28, 2017 Meeting

Preliminary Matters

- **Scope & Form** –
  - Scope -- IdM alone ***or*** IdM + Trust Services
    - Trust Services = the creation, verification, and validation of electronic signatures, electronic seals, electronic time stamps, electronic registered delivery services, etc.)
  - Form -- not discussed or agreed (e.g., guidelines, model law, convention)
- **General principles**
  - Party autonomy -- freedom of contract
  - Non-discrimination -- legal effect and admissibility not denied solely on the grounds that identification was made in electronic form
  - Technology neutrality
  - System model neutrality
  - Functional equivalence – [but questioned]
- **Relationship of IdM law to** –
  - Privacy law
  - Security law

UNCITRAL – IdM Project
Discussions at April 24-28, 2017 Meeting

Possible Substantive Topics - 1

- **Legal Recognition**: i.e., when does credential satisfy legal obligation? When can RP rely for compliance? IdM to satisfy legal requirements for identification
- **Mutual Recognition**; i.e., acceptance of identity credentials created in one IdM system by another IdM system regardless of the use of different technology, rules or business model
- **Attribution of identity information to a subject**:
  - determination that the person using the identity credential was the person purported to be; and
  - how a relying party could carry out that determination
- **Reliance:** when is reliance by RP appropriate?

UNCITRAL – IdM Project
Discussions at April 24-28, 2017 Meeting

Possible Substantive Topics - 2

- **Levels of Assurance**
  - And presumptions / legal benefits depending on LOA
- **Liability/Risk allocation**
- **Transparency:**
  - Duty to disclose processes and methods to deliver IdM services
  - Duty to discloses breaches
- **Conclusion**:
  - "The Working Group **agreed that the notions of legal recognition, mutual recognition, attribution, reliance, liability and risk allocation, and transparency** were relevant for its work on IdM and trust services and suggested that those notions should be further considered, . . . at a future session."

Uniform Law Commission

Uniform Law Commission
The National Conference of Commissioners on Uniform State Laws

- 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), adopted in all 50 states
  - Uniform Electronic Transactions Act (UETA), adopted in 47 states
- Drafting committee meetings open to the public

Uniform Law Commission – Project to Develop U.S. Domestic Law Governing IdM

- Study Committee appointed to consider desirability of developing a Uniform Act on Identity Management in Electronic Commerce
- 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
- Began work in August 2016 -- Struggling to define
  - need for legislation, and
  - topics to be addressed

Key Recent Legal Developments

(at Level 3 - System-Specific Rules)

Level 3 System-Specific Rules Definition and Role of a Trust Framework

- OIX Trust Framework Definition Project
- To be discussed this afternoon
- Role of a Trust Framework
- Form of trust framework
  - Contract-based vs regulatory-based
- Legislation vs. Trust Frameworks

Level 3 System-Specific Rules Trust Framework Forms

- Private Sector Rules (contract)
  - SAFE-BioPharma Operating Policies
  - CA/Browser Forum Guidelines
  - InCommon Operating Policies and Practices
  - CertiPath Certificate Policy

- Public-Private Partnership Rules (contract)
  - UK: GOV.UK Verify program
  - US: Connect.gov program (inactive)

- Public Sector Rules (laws/regulations)
  - EU: eIDAS Regulation
  - Florida: Identity Management Rule (New)
  - Estonia IdM law

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

Florida Agency for State Technology Identity Management Regulation

- Proposed rule
- Establishes rules for use of State IT resources
- Requires identification of all state owned IdM resources
- Requires that state agencies must be capable of accepting external users authenticated by third-party IdPs who comply with specified standards
- Addresses privacy and security

IdM Legislation & Trust Frameworks - A Workable Solution?

- How can/should they work together?
- Will they enable and facilitate – or inhibit – development of a sustainable and interoperable identity ecosystem?
- What approach should they take?
- How far should Level 2 general identity management law go?
  - What issues should it address?
  - Which issues should be left to the parties to contractually define in Level 3 System-Specific Rules?
  - How prescriptive should it be?
- Where do Principles of Identification fit in?

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

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)

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

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

Other –

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 trans-boundary 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