Liability and Participant Obligations

The Means for Building Trust?

Thomas J. Smedinghoff

UNCITRAL Colloquium on Legal Issues Related to Identity Management and Trust Services

Vienna April 21-22, 2016
The Question Everyone Asks

What’s My Liability?
Some of the Liability Concerns

- **Identity Provider**
  - Incorrectly identifying or authenticating a user
  - Issuing an erroneous identity credential
  - Failing to verify or revoke a credential
  - Failing to protect (or misusing) a user’s personal data

- **Relying Party**
  - Relying on a false identity credential
  - Failing to protect (or misusing) a user’s personal data

- **User / Data subject**
  - Providing false identity data
  - If someone else uses the user’s credential
  - If someone misuses the user’s personal data
The Impact of Liability on an Identity System

- Liability is a **barrier** to participation.

- Liability also has functional characteristics. It provides a means to –
  - allocate risk among participants
  - enforce obligations of participants
  - punish non-compliance and compensate injured parties

- Liability is a **zero-sum game**!
Liability Flows From Duties

- Generally, **Party A is liable to Party B only if** –
  - Party A **owes a duty** to Party B,
  - Party A **breaches** that duty, and
  - Party B **suffers damage** as a result of Party A’s breach

- **Sources of duties**
  - Laws or regulations (public law)
    - Typically general law that is not identity-specific
    - Often leads to uncertainty re duties and liability
  - Contracts among the parties – e.g., system rules (private law)
    - Typically specific to each identity system
    - Often incompatible with other identity systems

- Let’s consider the legal framework governing identity system duties and liabilities – starting with the credit card analogy
Identity Systems Are Analogous to Credit Card Systems

- Large multi-party systems
- Often international in scope
- Many participants in multiple roles, including -
  - many data subjects / [cardholders]
  - many identity providers / [card issuing banks]
  - many relying parties / [merchants]
- Any participant can transact with any other participant
  - often on a random one-time or very infrequent basis, and
  - without a direct contractual relationship
- The system supports stranger-to-stranger transactions
Data Flow: Multiple Banks issue credit cards to multiple cardholders (Users) who use those cards to make purchases from multiple Merchants
Interactions of a Multi-Party Credit Card System (with validation)

Data Flow: Each Merchant (in this case, Merchant_3) must then contact the applicable bank (red lines) to verify validity of credit card being used for each transaction.
Interactions of a Multi-Party Identity System

Data Flow: Multiple IdPs issue identity credentials to multiple users who use those credentials to facilitate online transactions with multiple RPs
Interactions of a Multi-Party Identity System (with validation)

Data Flow: Each Relying Party (in this case, RP_3) must then contact the applicable Identity Provider (red lines) to verify validity of credential being used for each transaction
Multi-Party Systems Require System Rules

- System rules define the business, technical, and legal rights and obligations of all of the participants
  - Often called a “trust framework,” “scheme rules,” or “operating rules,”

- Enforceable “System Rules” are necessary so that . . .
  - The system **functions properly** – i.e., the system “works”
    - Everyone needs to know what to do
  - The system is considered **trustworthy** by all participants

- Because both identity and system rules are **relative**, system rules will vary widely
  - E.g., compare “UK.GOV Verify” rules with “Facebook” rules
Topics Often Covered by System Rules Include . . .

- Identity proofing
- Credential issuance
- Levels of assurance
- Credential use
- Reliance on a credential
- Credential authentication
- Credential maintenance and lifecycle management
- Revocation of credentials
- Privacy of user data
- Security of user data and authentication processes
- Technical specifications (e.g., credential contents & format)
- Certification; Audit and assessment oversight
- Legal – warranty, liability, governing law, dispute resolution
System Rules Affect All Participants & Transactions Within an Identity System
Identity System Rules Are Subject to: Legal Duties Imposed by General Law

1. **Existing General Law (State level)**

   - Contract law, Tort law, Commercial law, Privacy law, Fraud law, Competition law, etc.

2. **System Rules must comply with Level 1 law above**

   - **Public Law**
   - **Private Law (Contract)**

   - Identity System 1
   - Identity System 2
   - Identity System N
Identity System Rules Are Subject to: Legal Duties Imposed by General Law

1. **Existing General Law**
   - (State level)
   - **Problems!**
     - Legal barriers; legal uncertainty re duties; unclear or inappropriate liability allocation; lack of uniformity; etc.

2. **System Rules**
   - must comply with Level 1 law above

- **Public Law**
  - **Problems!**
    - Lack of trust; lack of interoperability; barriers to mutual recognition; need to incentivize; etc.

- **Private Law (Contract)**
  - **System Rules**

**Existing General Law**
- Contract law,
- Tort law,
- Commercial law,
- Privacy law,
- Fraud law,
- Competition law, etc.

**System Rules**
- Identity System 1
- Identity System 2
- Identity System N
New Identity System Legal Framework: Duties Imposed on Three Levels

1. **Existing General Law** (State level) - Contract law, Tort law, Commercial law, Privacy law, Fraud law, Competition law, etc.


System Rules must comply with Levels 1 and 2 above

3. **Identity System**
   - Identity System 1
   - Identity System 2
   - Identity System N

Public Law

Private Law (Contract)

System Rules
Many Challenges for Identity Legislation, such as . . .

- What duties should the law impose?
- Do we focus on specific methodologies or outcomes?

- Where do we draw the line between public law and contract-based system rules?
  - What should be covered by law?
  - What should be covered by individual system rules?
  - In which cases should private contract-based rules be allowed to override public law rules?

- Where is liability addressed? How much can participants limit liability?
Virginia Approach

- **Applicable to** –
  - All identity systems
  - Identity providers only
  - All identity system transactions

- **Focuses primarily on** –
  - Liability

- Identity providers ARE LIABLE for --
  - Failure to comply with the standards set by the State of Virginia, and
  - Failure to comply with any contractual agreement or the trust framework for the identity system of which they are a part

- Safe harbor -- Identity providers are NOT LIABLE if they do not comply with foregoing
EU – eIDAS Approach (1)

- Applicable to -
  - EU Member state identity systems that opt-in (i.e., notify)
  - Identity providers and public sector relying parties
  - Public sector transactions only
  - Inter-identity system transactions only

- Focuses primarily on -
  - Mutual recognition of credentials for public services
  - Imposition of credential issuance obligations
  - Liability for failure to comply

- Relying party obligations:
  - Each member state obligated to recognize identity credentials issued by other member states that have opted-in (notified)
Identity provider obligations:

- **Member state** is obligated to -
  - Ensure that data uniquely representing a person is attributed to that person, in accordance with specifications and implementing acts, at the time the credential is issued
  - Ensure availability of online authentication system

- **Party issuing credential** is obligated to -
  - Ensure that the credential is attributed to proper person in accordance with specifications and implementing acts

- **Party operating authentication system** is obligated to –
  - Ensure the correct operation of the authentication procedure

- Each party liable for failure to do foregoing, whether negligent or intentional
So How Might UNCITRAL Address Duties & Liability?

- Recognize that there will be many identity systems
  - Recognize that duties and liability are relative
  - Focus on identity system neutrality
- Consider applicability
  - All Identity systems vs. inter-system transactions
  - All roles vs. selected roles
- Consider goals, such as –
  - Incentivizing identity system marketplace
  - Removing barriers
  - Ensuring certainty and predictability of legal rules
  - Providing mechanisms to promote trust and interoperability
  - Facilitating cross-border transactions
  - Providing appropriate incentives
- Focus on outcomes rather than prescribing specific processes
Thomas J. Smedinghoff
Privacy & Cybersecurity Practice Group
Locke Lord LLP
111 S. Wacker Drive
Chicago, Illinois 60606
+1.312.201.2021
Tom.Smedinghoff@lockelord.com