RSACONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

# Deciphering the Legal Framework that Governs Online Identity Systems

SESSION ID: LAW-W04A

Thomas J. Smedinghoff

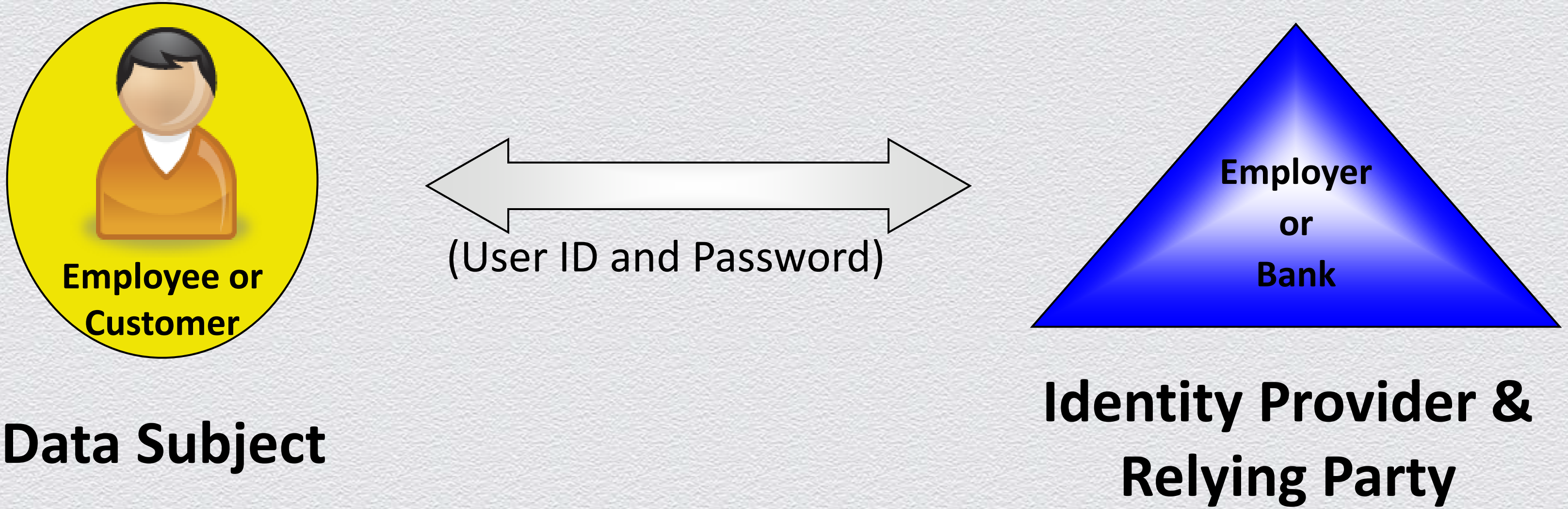
Partner
Edwards Wildman Palmer LLP
Chicago, Illinois

TSmedinghoff@EdwardsWildman.com
@smedinghoff

# Focus - Multi-Party Online Identity Systems

- Sometimes called “federated” systems
- Involves relying on identity assertions from third parties

# Traditional Two-Party Approach



Employee or Customer

(User ID and Password)

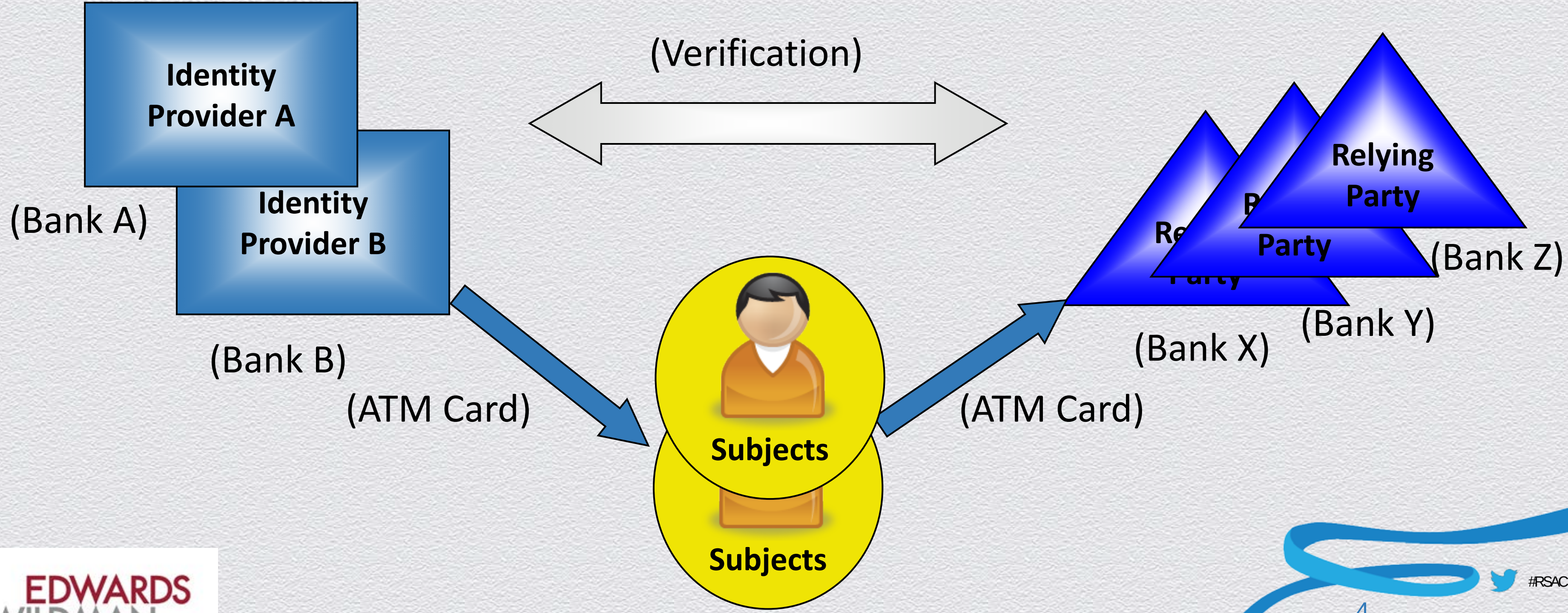
Employer or Bank

Data Subject

Identity Provider & Relying Party

# The Developing Multi-Party Approach: Federated Identity Systems

ATM Example



# The Role of Rules

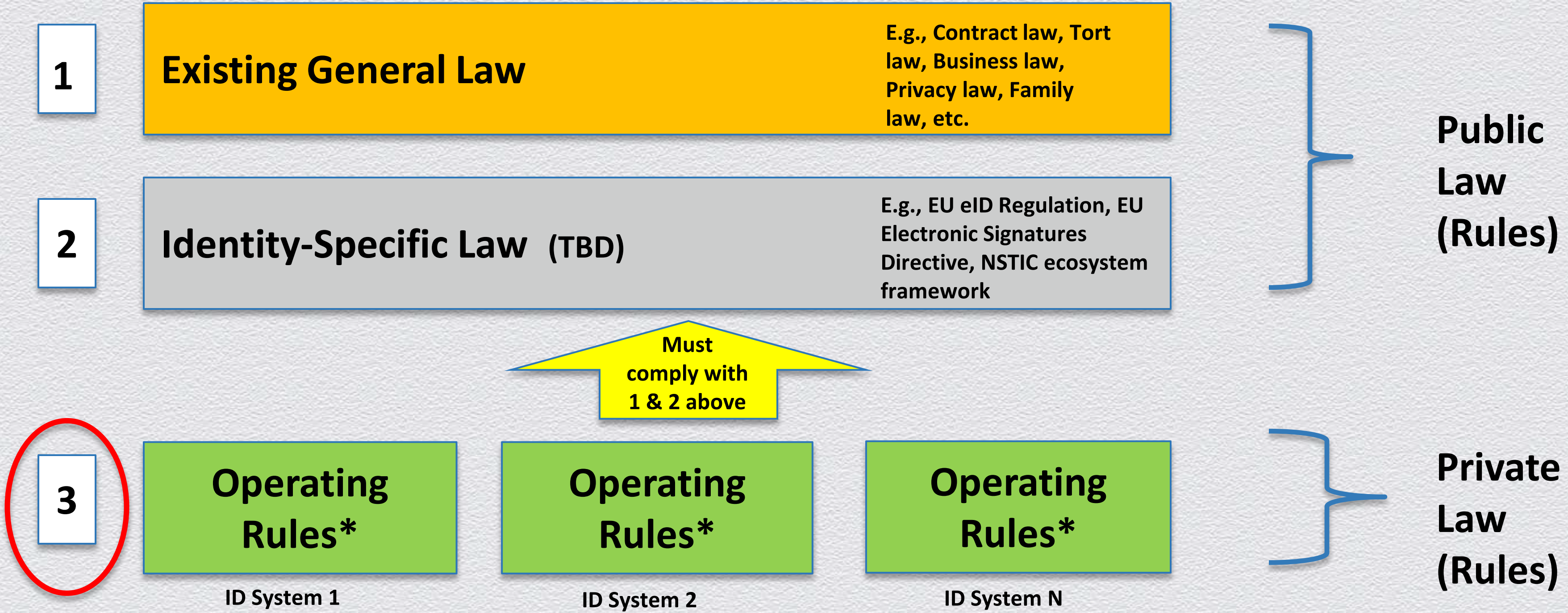
- All Multiparty Systems Need Rules
  - Identity systems
  - Electronic payment systems
  - Credit card systems
  - Other systems

- Purpose of Rules
  - Make it work – from a functional perspective
  - Make it trustworthy – willingness to participate
  - Define & govern the legal rights and responsibilities of the participants
  - Minimize abuses

# Two Types of Rules Govern Identity Systems

- Public Rules
  - Written by: governments
  - Consist of: law – i.e., statutes, regulations, common law, court decisions
  - Apply to: everyone
  - Typically not identity-specific
- Private Rules
  - Written by: private parties
  - Consist of: Technical specifications, standards, policies, processes, contracts
  - Apply to: only those who have agreed to them (by contract or conduct)
  - Must comply with public rules (i.e., law)
  - Typically written for (and unique to) a specific identity system

# Three Levels of Rules Govern Identity Systems



1

**Existing General Law**

E.g., Contract law, Tort law, Business law, Privacy law, Family law, etc.

2

**Identity-Specific Law (TBD)**

E.g., EU eID Regulation, EU Electronic Signatures Directive, NSTIC ecosystem framework

Must comply with 1 & 2 above

3

**Operating Rules***

ID System 1

**Operating Rules***

ID System 2

**Operating Rules***

ID System N

Public Law (Rules)

Private Law (Rules)

* a/k/a System Rules, Trust Framework, etc.

# Level 1: Existing General Law

- Characteristics
  - Public law (comes from the government)
  - Includes statutes, regulations and common law (court-made law)
  - Applies to everyone
  - Currently exists
  - Enforced by courts at the state and/or country level
- Issues
  - Not designed for identity transactions – may not be a good fit
  - Not always clear how it applies to identity; applicability may be ambiguous
  - Can vary from jurisdiction to jurisdiction

# What's in Level 1 Existing General Law?

- All existing law – whether relevant to IdM or not
  - Examples include -- commercial law, family law, tax law, export control law, real property law, tort law, contract law, healthcare law, food & drug law, environmental law, labor law, advertising law, etc.
- Some Level 1 existing law may apply to IdM systems, such as --

Privacy law
Data security law
Contract law
Consumer law
Tort law re negligence, fraud, etc.
Law of defamation

E-transaction / e-signature law
Law regulating encryption
Rules of evidence
Warranty law
Law of negligent misrepresentation

EDWARDS WILDMAN

# Level 2: Identity-Specific Law

- Characteristics
  - Public law (enacted by legislatures or regulators)
  - Designed specifically for identity transactions – e.g., rules for IdPs
  - Applies to multiple identity systems
  - Enforced by courts at the state and/or country level
- Issues
  - Level 2 largely non-existent (but many efforts to develop legislation)
  - Efforts to develop it may get it wrong
  - Can vary from jurisdiction to jurisdiction

# What's in Level 2 Identity-Specific Law?

- (Mostly) New laws focused specifically on identity systems
  - Applicable to all identity systems within scope
- Examples of Level 2 law include –
  - EU eID Regulation (proposed draft)
  - EU E-Signatures Directive (re credential service providers)
  - Digital signature laws (e.g., Washington, Illinois, Malaysia, Egypt, etc.)
  - NSTIC Identity Ecosystem Framework (proposed as voluntary rules)
- Analogous examples of Level 2 law include –
  - Regulation Z (governing all credit card systems)
  - Regulation E (governing all consumer funds transfer systems)

# Level 3: Operating Rules / Trust Framework

- Characteristics
  - Private law
  - Written specifically for a particular identity system
  - Applies only to participants in that system that agree to be bound
  - Prepared by one or more participants in a specific system
  - Made enforceable by contract; Enforced by courts (under law of contract)
- Issues
  - Can vary from identity system to identity system – inhibiting interoperability
  - Of no value unless participants agree to them
  - Cannot violate Level 1 or Level 2 public law
  - Must address jurisdictional conflicts

# What's in Level 3 Rules?

- Detailed rules developed specifically for a particular identity system
- Examples of Level 3 rules (for a specific identity system) include –
  - TSCP Common Operating Rules
  - FICAM Trust Framework
  - SAFE-BioPharma Operating Rules
  - Facebook Connect rules
- Analogous examples of Level 3 rules include –
  - Visa Operating Regulations (for a specific credit card system – i.e., Visa)
  - NACHA Operating Rules (for a specific funds transfer system – i.e., ACH)

# Building a Legal Framework: How You Can Control the Applicable Law

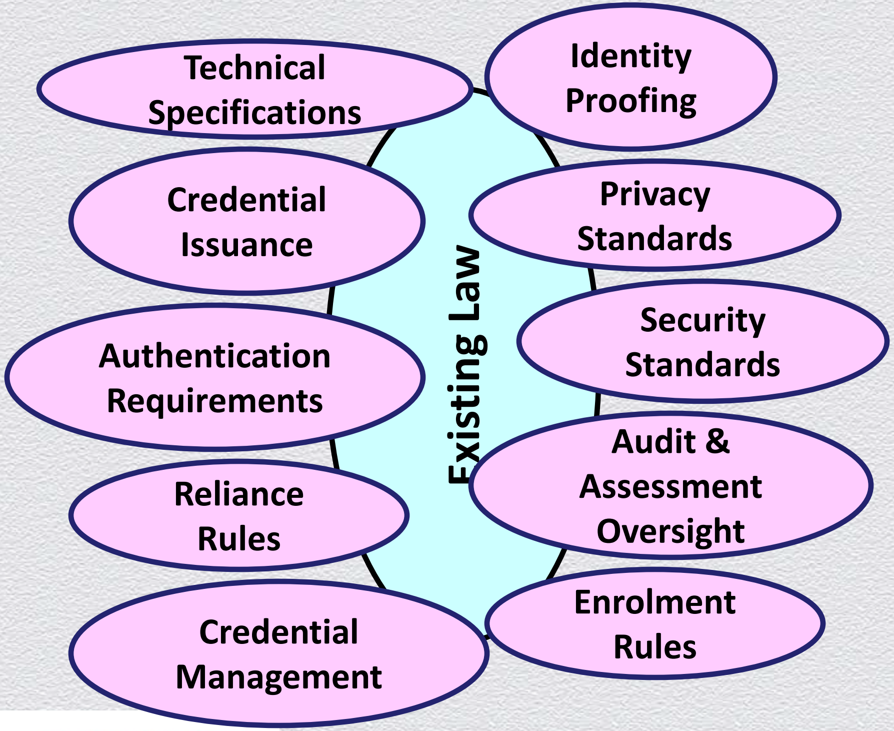
- You must comply with Level 1 and 2 public law, **but . . .**
  - Much of that law is designed as a gap-filler – i.e., it applies only if you don’t agree on something different
- At Level 3 (Private rules) --
  - Parties are free to –
    - Modify Level 1 and 2 rules, and
    - Agree on whatever additional rules they want
  - So long as they don’t violate any Level 1 or 2 laws in the process
- So the key to structuring the rules for an identity system is to design a comprehensive set of private rules
  - What isn’t covered at Level 3 will default to Level 1 & 2

# Operating Rules / Trust Framework

Operating Rules / Trust Framework is a set of documents developed for the operation of a specific identity system, consisting of:

- ***Business, Technical and Operational Rules and Specifications*** that:
  - define the requirements for proper operation
  - define the roles and operational responsibilities of participants, and
  - provide adequate assurance regarding the accuracy, integrity, privacy and security of its processes and data, and
- ***Legal Rules*** that:
  - make the Business, Technical and Operational Rules legally binding on and enforceable against the participants, and
  - define and govern the legal rights, responsibilities, and liabilities of the participants of the identity system.

# Business & Technical Rules: (Components Necessary to "Make it Work")



Partial listing of Business & Technical Rules

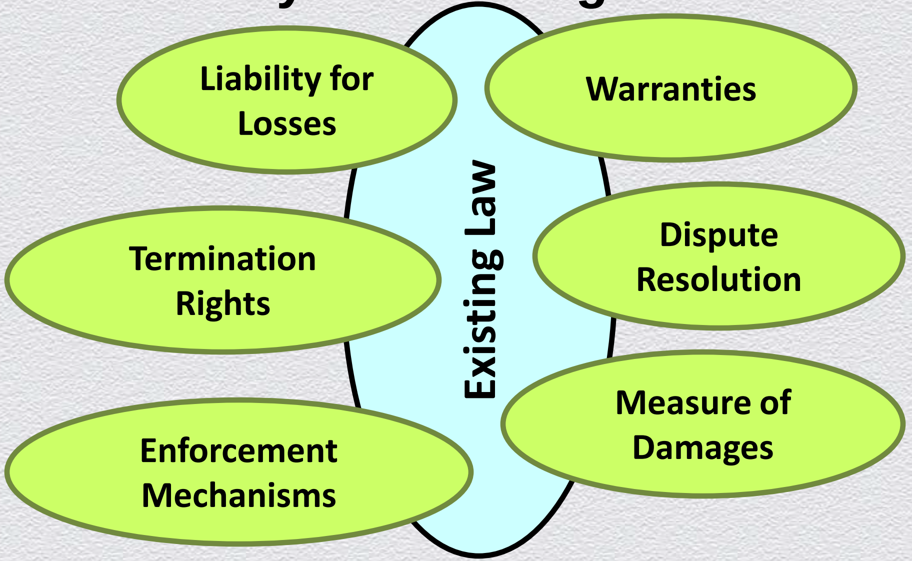
NOTE: Must comply with any existing law;

Also may be supplemented by existing law

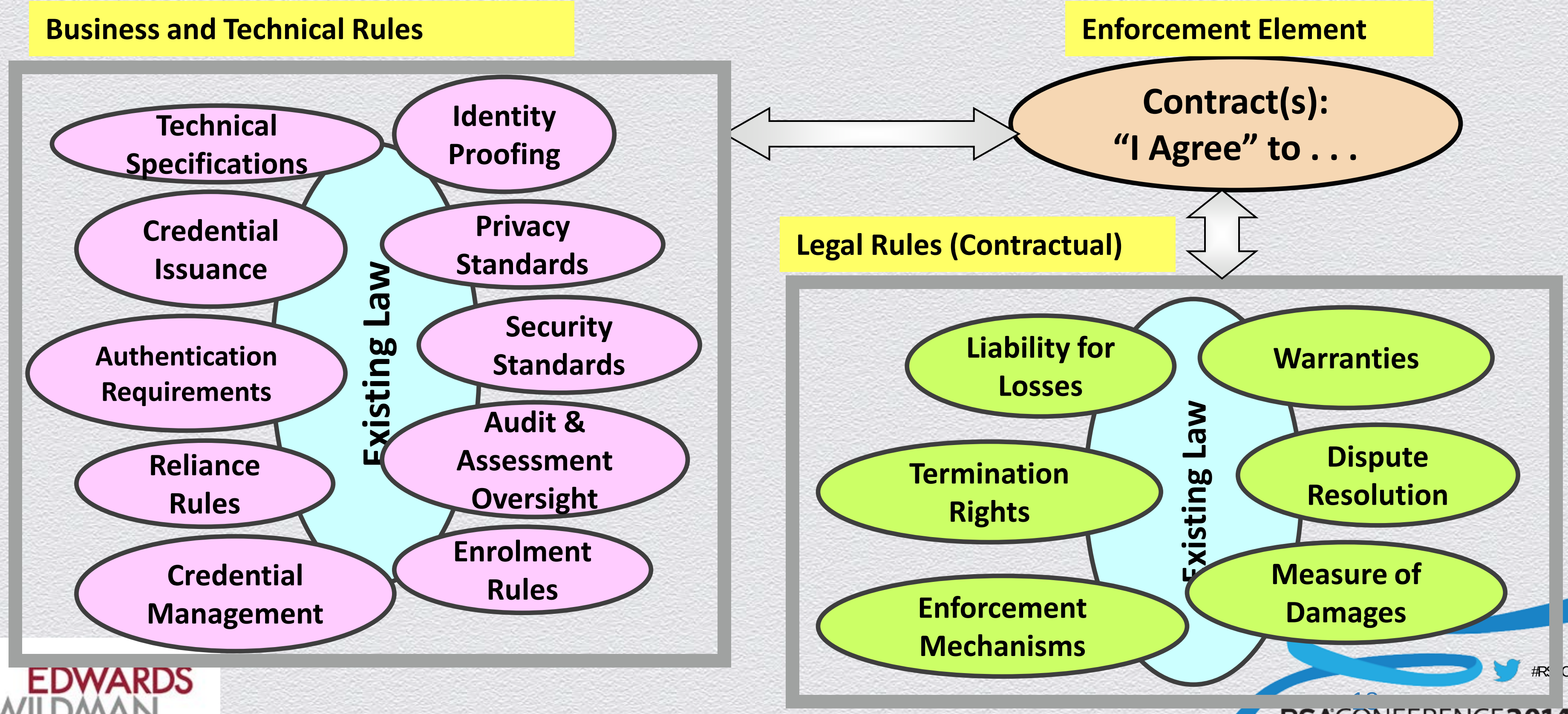
# Legal Rules (contract-based) (To Govern Legal Rights of the Parties)

Partial listing of Legal Rules

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



# Put It All Together with a Contract to Form Enforceable "Operating Rules"



Business and Technical Rules

Existing Law

Technical Specifications

Identity Proofing

Credential Issuance

Privacy Standards

Security Standards

Authentication Requirements

Audit & Assessment Oversight

Reliance Rules

Enrolment Rules

Credential Management

Enforcement Element

Contract(s): "I Agree" to . . .

Legal Rules (Contractual)

Existing Law

Liability for Losses

Warranties

Termination Rights

Dispute Resolution

Enforcement Mechanisms

Measure of Damages

# The Operating Rules Are the Key to Defining the Legal Framework

- Operating rules define and control most of the legal risk.
  - They provide the identity-specific rules that make the system work
  - They specify the rights and obligations of the parties
  - They specify the duties that form the basis for liability
  - They can also be used to control the liability of each party
- Developing appropriate operating rules is critical!

# Questions?

**Thomas J. Smedinghoff**

**Edwards Wildman Palmer LLP**

**Chicago**

**TSmedinghoff@edwardswildman.com**