American Bar Association

Federated Identity Management Legal Task Force

Thomas J. Smedinghoff
Wildman, Harrold, Allen & Dixon, LLP
Chicago

Co-Chair, ABA Federated Identity Management Legal Task Force

Background

Wildman Harrold
Attorneys and Counselors

- ABA Task Force established January 2009
- Co-Chairs
  - Thomas J. Smedinghoff, Wildman, Harrold, Allen & Dixon LLP
  - Jane K. Winn, University of Washington School of Law
- It's an open project. Participants include:
  - Lawyers, non-lawyers, IdM technology experts, businesspersons, and other interested persons
  - From businesses, associations, and government agencies
  - From U.S., Canada, EU, and Australia so far
- Website (and sign up for listserv) at –
  - **www.abanet.org/dch/committee.cfm?com=CL320041**
  - Alt. URL: **http://tinyurl.com/yft89m8**

Goals

Wildman Harrold
Attorneys and Counselors

- Identify and analyze the **legal issues** that arise in connection with the development, implementation and use of federated identity management systems;
- Identify and evaluate appropriate **legal models** to address issues;
- Develop **model terms and contracts** that can be used by parties

Work Groups

Wildman Harrold
Attorneys and Counselors

- Definitions
- Legal issues
- Privacy
- ID Proofing / Notaries
- Legal structures
- Model Contracts

Interim Projects Include . . .

Wildman Harrold
Attorneys and Counselors

- Liability for what? – Identify what could go wrong
- Identify existing laws related to identity management
- Identify potential liability models
- ID Proofing – Impact on legal issues
- Notaries as ID proofers
- Common definitions
- Levels of Assurance – Impact on legal issues
- Collecting sample contracts

Legal Landscape – The Rules

Wildman Harrold
Attorneys and Counselors

- Private rules created by or for the participants –
  - e.g., performance obligations of the participants
- Preexisting statutory/regulatory rules that impact performance of participants in the IdM system
  - E.g., privacy laws, security laws, FFIEC, etc
- Preexisting legal rules (statutes, regulations, common law) that impact liability of participants in the IdM system
  - E.g., warranty law, negligence law, etc.
- Sometimes private rules and existing laws clash

Why Do We Care About Legal Issues?

Wildman Harrold
Attorneys and Counselors

- We need to create a legal framework to make it work
  - Need rules to ensure participant performance of obligations necessary to make it work
  - Need ability to enforce those rules
- We need to understand impact of existing laws
  - We need to understand how existing law will determine liability when losses occur
  - What laws we can change by contract (and how)
  - What laws we can't change, and must comply with
  - Need to understand how to legally mitigate risks and allocate liability
- Need enforcement mechanism

Consider the Sources of the Legal Issues

Wildman Harrold
Attorneys and Counselors

- Statutes and regulations (in all relevant jurisdictions)
- Common law / judicial decisions
- Standards
  - Industry associations (e.g., PCI DSS)
  - System rules – e.g., Visa rules, ATM system rules
- Self-imposed requirements
  - Unilateral undertakings, such as privacy policy or CPS
- Contracts among the parties
  - Trust frameworks
  - Bilateral agreements

Consider Categories of Law

Wildman Harrold
Attorneys and Counselors

- Contract law
- Warranty law
- Tort law
  - Negligent performance
  - Negligent misrepresentation
  - Fraudulent misrepresentation
  - Defamation
- Third party beneficiary law
- E-transactions law
- Consumer protection law
- Security law
- Privacy / data protection law
- Identity theft law
- Antitrust law
- Unfair competition law
- False endorsement
- False advertising
- IP law
  - Copyright law
  - Trade secrets law
  - Trademark law
  - Patent law
- Statutory/regulatory law
  - Governing the IdM process
  - Imposing IdM compliance obligations
- Liability for the conduct of others
- Governmental immunity law
- Other

Consider Factors that Affect Application of the Law

Wildman Harrold
Attorneys and Counselors

- Nature of the person involved
  - e.g., Individual, consumer, business, corporate entity, government entity
- Expertise of the person involved
  - e.g., unsophisticated vs. professional / in the business, etc.
- Nature of the information involved
  - e.g., sensitivity of personal information (e.g., name vs. SSN)
- Nature of the use involved
  - e.g., login to garden club website vs. launch nuclear missiles
- Nature of any resulting harm
  - e.g., embarrassment, economic loses, property damage, personal injury
- Level of assurance involved

Other Factors

Wildman Harrold
Attorneys and Counselors

- Who created the legal rule?
  - The participants – e.g., contracts?
  - Government statutes or regulation?
  - Court decision – common law?
- Where does the legal rule apply?
  - What jurisdiction's law controls transaction?
  - How to handle cross jurisdiction transactions?
- How can we change the legal rule?
  - Can statutes, regulation, or common law be varied by contract?
  - What happens when laws conflict between jurisdictions?

Some Possible Approaches to the Legal Analysis

Wildman Harrold
Attorneys and Counselors

- Focus on obligations and concerns of each role
  - E.g., what is the IdP obligated to do to make it work?
  - E.g., what is the IdP concerned about re performance by others?
- Focus on actions that occur at each point in the IdM process
  - E.g., for issuance of credential . . .
    - What could go wrong and give rise to liability?
    - What are potential liabilities of each participant (IdP, Subject, Relying Party, etc.) that could flow from such an action?
- Focus on categories of legal risk
  - E.g., performance risk, privacy risk, security risk, identification risk, technology risk, authentication risk, etc.

For Example . . .
Consider Legal Issues By Role

Wildman Harrold
Attorneys and Counselors

- Basic roles include –
  - Trust Framework Provider / Assessor / Auditor
  - Subject / Identity Provider / Relying Party
  - Victim (non-participant)
- For each role in an IdM system, consider the following:
  - What are the obligations required of a participant in that role in order to make the IdM system work properly
  - What are the concerns that a participant in that role has re participating in and relying on the IdM system?
  - What rights does that role have by law?
  - What other rules are necessary, or should be addressed, for a participant in that role?

Recognize That "Liability" Per Se Is Not the Issue

Wildman Harrold
Attorneys and Counselors

- "Liability" is just the penalty when you, or someone else, does something wrong
- We need to define when something is wrong
  - What are you required to do?
  - What are you prohibited from doing?
  - What are you committing to (e.g., representations)?
  - What standard is applied to your conduct?
- We need to identify the legal issues of concern
  - We can't address the issue unless we know the potential source of the liability – e.g., warranty, antitrust, tort, contract, duty to authenticate, etc.
- We need to consider mitigation strategies

Some Liability Models

Wildman Harrold
Attorneys and Counselors

- DMV model – no IdP liability; other roles bear risk
- Credit card model – no Subject liability; other roles bear risk
- Contractual model – negotiated risk allocation
- Strict liability – regardless of fault
- Liability caps model
- EV SSL model – restrictions on ability of IdP to limit liability
- Warranty model – focus on guarantees
- Tort model – focus on standards of conduct; negligence

Common Problems to Consider

Wildman Harrold
Attorneys and Counselors

- The non-waivable statute problem
  - Some laws impact IdM systems
  - Can’t be changed by contract
- The cross-border problem
  - Addressing the problem of differing legal regimes
  - Requirements in one jurisdiction may not exist in another
  - Requirements in one jurisdiction may conflict with requirements in another

Addressing/Controlling Legal Issues

Wildman Harrold
Attorneys and Counselors

- Some legal issues cannot be controlled
  - Law governs – cannot be altered; must comply
  - So must understand impact
- Some legal issues can be controlled by contract
  - Law governs, but can be altered by contract, or
  - No law, so parties can determine by contract or other method
- For some legal issues its unclear whether the issue can be controlled
  - Governing law cannot be altered in some jurisdictions, but can be altered (or doesn't exist) in others
    - E.g., SSN transfer must be encrypted in some jurisdictions, but not regulated in others
    - E.G., Consent to transfer of personal data valid in some jurisdictions, not valid in others

Approaches to a Legal Framework

Wildman Harrold
Attorneys and Counselors

- Legislative/Regulatory framework
  - DigSig law in e.g., Washington, Malaysia, Egypt etc.
  - EU E-Signature Directive
  - But don't address all required issues
- Unilateral assertion model
  - E.g., original CPS approach
  - But can't ignore laws and regulations
- Contractual framework models
  - But can't ignore laws and regulations
- Hybrid framework – most likely

Further Information

Wildman Harrold
Attorneys and Counselors

Thomas J. Smedinghoff
Wildman, Harrold, Allen & Dixon LLP
225 West Wacker Drive
Chicago, Illinois 60606
312-201-2021
smedinghoff@wildman.com