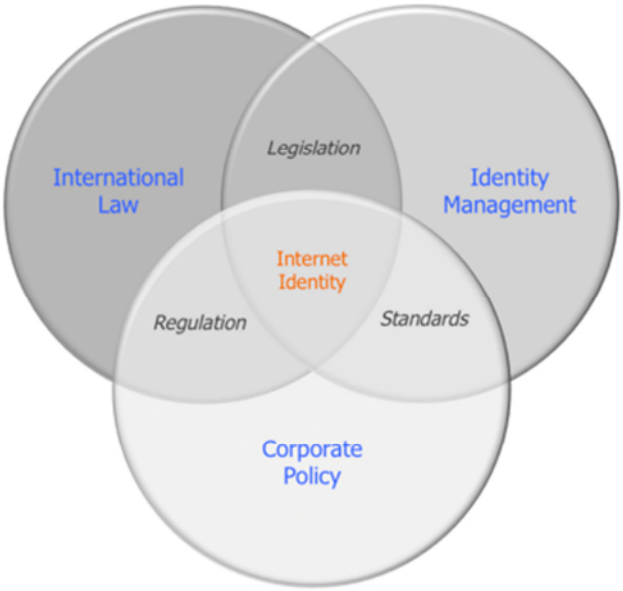
REPORT:

INTERNATIONAL IDENTITY LAW AND POLICY WORKSHOP

Identity Management Legal Task Force



REPORT: INTERNATIONAL IDENTITY LAW AND POLICY WORKSHOP

Thomas J. Smedinghoff
Chair, ABA Identity Management Legal Task Force

1. Introduction

The Open Identity Exchange, along with the American Bar Association's Identity Management Legal Task Force and The World Bank, hosted a legal and policy workshop on January 14, 2016 in Washington D.C. with the objective of discussing the main issues surrounding the adoption of identity management legislation.

Attendees were lawyers, business leaders, policy experts, and technologists representing a broad spectrum of public sector, private sector, and NGO leaders in identity. Participants also included experts involved in drafting the recently-enacted identity legislation in the EU and Virginia, and experts currently involved in planned and proposed upcoming legislative initiatives relating to identity management in both the U.S. and internationally.

The impetus for the meeting was several recent developments relating to identity management legislation. They included the following recently adopted identity management legislation:

- The European Union eIDAS Regulation adopted in 2014, and
- The Virginia Electronic Identity Management Act adopted in 2015;

and the following planned or proposed projects to develop new identity management legislation:

- The United Nations Commission on International Trade Law (International) project to develop international rules providing "a basic legal framework covering identity management transactions;"
- The Uniform Law Commission (United States) proposal to develop uniform identity management legislation for the 50 U.S. states; and
- The Virginia Identity Management Standards Advisory Council (Virginia) project to advise the Virginia Secretary of Technology on the identity management standards to be adopted as regulations in Virginia under its new Identity Management Act.

The goal of the meeting was to discuss the direction that such new identity management legislation should take, the issues it should address, and desired approaches.

A key theme reiterated throughout the event was the importance of focusing on outcome-based legislation. Participants voiced concern that legislation prescribing a specific technical process to implement identity standards would hinder innovation and ultimately prevent the success of a new legal regime.

This Report summarizes at a high-level the robust, thought-provoking and productive discussion in which the participants engaged.

2. The Identity Management Legal Framework

As background for the discussion, it was noted that federated identity systems, like most commercial multi-party transaction systems, are typically governed by three tiers of legal rules, consisting of a combination of public law and private law, as follows:

- Level 1 – General Law, including contract law, tort law, and privacy law across different jurisdictions;
- Level 2 – Identity Management-Specific Law, such as the recent EU eIDAS Regulation and Virginia legislation;
- Level 3 – Contract-based System Rules governing specific identity systems between parties.

Each level must comply with the levels below it. Level 1 and Level 2 are considered public law because they are enacted by governments (e.g., legislation or regulation) and thus apply to all within their scope. Level 3 is considered private law because it is a set of rules contractually agreed to by the parties in a specific identity system, and apply only in the context of that identity system. These three levels represent the legal environment in which each identity system operates. The details of this structure can be seen below in Figure 1.

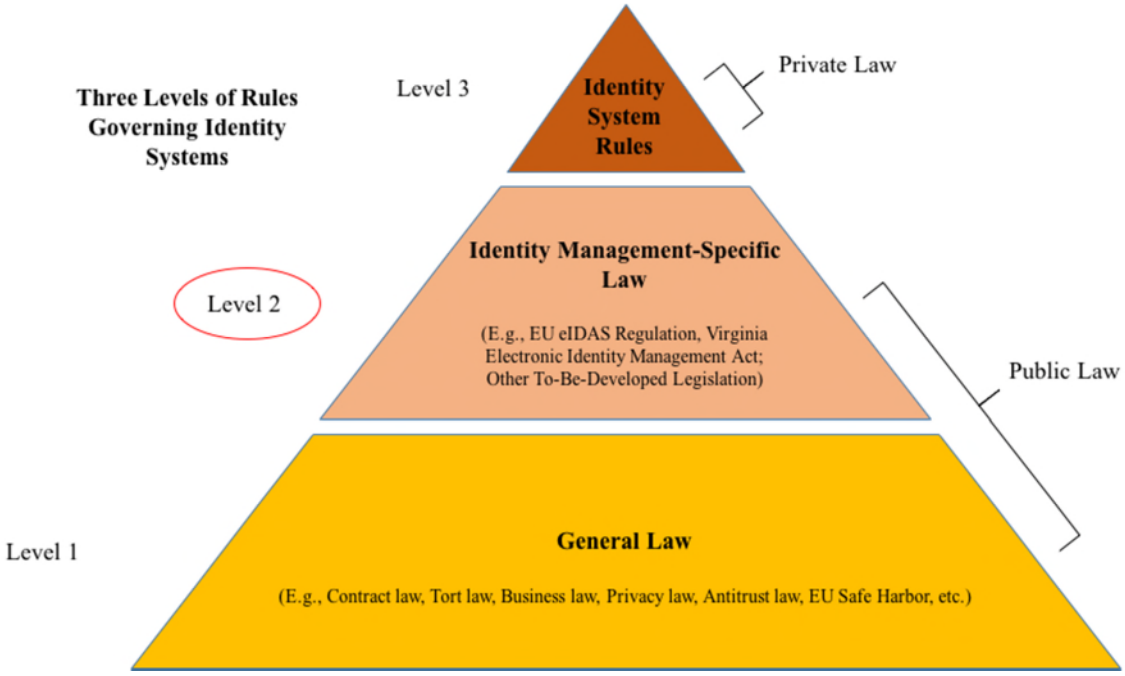


Figure 1: Three Levels of Legal Rules Governing Identity Systems

The objective of the workshop was to focus on the direction and approach of potential Level 2 legislation governing identity management. Individuals involved in the drafting of existing Level 2 legislation -- the EU eIDAS Regulation and the Virginia Electronic Identity Management Act -- participated in the event and provided invaluable insight into the goals and approaches of those two legislative initiatives.

3. Discussion

Attendees participated in moderated discussions covering five general topics in order to foster a dialogue surrounding Level 2, Identity Management-Specific Law. The topic categories were:

1) Trust, Acceptability, Interoperability, and Enforcement;
2) Liability;
3) Privacy and Security;
4) Business and Technical Standards;
5) Participant Obligations and Related Issues.

Participants expressed differing viewpoints on the type of legislation that might be needed, but did reach a general consensus that overly-prescriptive legislation would stifle technical innovation and harm the ultimate goal of promoting trust in identity transactions. Thus, an overarching theme for the day was how to create legislation that is outcome-focused as opposed to prescriptive.

(a) Trust, Acceptability, Interoperability, and Enforceability

The first moderated discussion focused on trust, acceptability, interoperability, and enforceability. The participants were presented with the following questions to guide their discussion on this topic:

- What is the best legislative mechanism for addressing trust concerns?
- Should legislation define legal requirements for trust, or trust levels?
- Should legislation define legal requirements for legal acceptability and effectiveness?
- How should legislation address cross-system and cross-border legal interoperability?

The discussion quickly focused on the question of whether or not it is possible for legislation to establish trust, or alternatively, how legislation can be designed to enable an environment in which trust is likely to occur.

Initial discussion centered on the European Union's eIDAS Regulation. eIDAS does not include language specific to the creation of trust, but instead addresses trust by focusing on outcome-based standards for levels of assurance and a peer review process that is designed to ensure that member state identity systems meet the required levels of assurance. The use of these standards ensures that the individual national policies will promote interoperability through mapping and notification of compliance.

It was also noted that the creators of eIDAS recognized that overly burdensome legislation would stifle innovation in a highly technical identity economy. As a result, eIDAS includes a method for change through cooperation. Participating states can notify each other of changes in technology or standards that may harm or hinder the existing rules for interoperability. Participating technical experts can quickly evaluate and remediate these changes as necessary to ensure that legislative gridlock does not prevent the adaptation of the eIDAS standards.

Participants discussed how the eIDAS program did not specifically mandate trust, but sought to establish an environment where independent member states could trust other state systems through mapping to common levels of assurance. This reiterated the importance of the day's theme of outcome focused legislation. The eIDAS approach seeks to define an outcome without defining the process for achieving that outcome. In doing so, eIDAS is intended to promote innovation and trust between participating member states.

The outcome itself was also discussed as an important part of any legislation. Many participants felt that the goal of legislation should be able to establish trust through the reliability and repeatability of identity transactions with an openness of standards. Openness was considered uniquely important given the numerous parties participating in identity transactions. The OIXnet registry of trusted identity systems was cited as an example that enables increased transparency and adoption through exposure. Much like the eIDAS program, participating parties are more likely to trust their counter-parties when the systems in which they operate are open and understandable.

Finally, with regard to the topic of interoperability, it was noted that cross-border interoperability of identity credentials and identity assertions does not necessarily require harmonization of standards and laws between the applicable countries. For example, it was noted that the eIDAS Regulation explicitly avoided harmonization in favor of allowing EU member states to develop identity systems best suited to their own citizens and transactions, and focused instead on ways to mutually accept identity credentials cross-border based on standards for the exchange of identity assertions and the interpretation of their quality through mapping to an agreed set of identity assurance levels.

(b) Liability

The second moderated discussion focused on the subject of liability. Participants were presented with the following questions to guide their discussion on the topic:

- Should liability be addressed by legislation?
- What is the appropriate policy for liability allocation?
- Is there a one-size-fits-all approach?
- How should identity management legislation address liability – domestically and in cross-border transactions?

The discussion recognized that parties to an identity transaction fulfill a variety of roles, such as identity provider, relying party, and data subject, and may involve a variety of participant types, including businesses and other private sector organizations, government agencies, and individual consumers. Moreover, an identity transaction may involve differing jurisdictions and uncertain legal rules. As a result, assessing liability risk in the event of an inaccurate identity credential, a data breach, or other event where damage occurs may be difficult at best. Thus, like trust, the uncertainty surrounding liability is a barrier for many participants.

Participants recognized that the issue of liability allocation is a difficult one, and the result may well vary depending on the type of parties involved. They also recognized that even in the absence of a Level 2 identity-specific rule governing liability, if someone suffered a loss and sued, a court would find some basis (presumably under Level 1 General Law) for allocating liability. But in that case, the problem is lack of predictability.

At the same time, it was also noted that liability is a zero-sum game. That is, insulating one party from liability in the case of a loss does not eliminate the harm – it just means that someone else must bear the loss. Thus, while liability-limiting rules may have the effect of protecting one party, they are more properly characterized as liability-allocating rules, as they simply determine which party must bear the loss.

It was noted that the Virginia Electronic Identity Management Act (VA law) attempted to create a standards-based reference point for court decisions on liability in identity transactions. That is, identity providers who complied with the standard to be adopted under the VA law would have a safe harbor from liability (i.e., relying parties would bear the risk), while identity providers that did not comply would bear the liability risk.

Conversely, eIDAS placed places liability risk with the government operating an identity system that it has notified, but defers to local country law for the parameters of such liability risk.

Because liability is often determined on a case by case basis, many participants felt that it would be difficult to include any specific provision for liability in legislation intended to be adapted to the growing and ever-changing identity market.

Recognizing the value of liability-limiting rules, however, reference was also made to the SAFETY Act, which provides important legal liability protections for providers of Qualified Anti-Terrorism Technologies - whether they are products or services. The goal of the SAFETY Act is to encourage the development and deployment of effective anti-terrorism products and services by providing liability protections. By implication, the question raised was whether something similar is needed to encourage the implementation of effective identity systems.

The issue of liability is also intimately connected with the rise of cyber-insurance. Participants pointed out that this emerging market is linked to the increased number of data breaches in the public and private sector. Any legislation that attempts to cap or define liability in the identity marketplace may impact the ability of any future insurance scheme to underwrite and protect clients from excessive damages.

Participants noted that any liability definitions must also be constructed to incentivize device manufacturers and other participating parties to recognize the risks associated with identity transactions.

Ultimately, liability is determined in the courts if no prior definition is defined in legislation. The question is then whether participants in the identity marketplace are willing to accept the risk of being found liable for injury as a result of their breach in the duty of care under existing law, or would prefer a more predictable (but perhaps less favorable) rule in identity-specific legislation.

(c) Privacy and Security

Next, the discussion considered on the need for addressing privacy and security issues in identity-management-specific legislation. Participants were presented with the following questions to guide their discussion:

- What is the appropriate policy for privacy protection?
- Should, or how should, identity management legislation address privacy?
- What is the appropriate policy for data security?
- Should, or how should, identity management legislation address data security?

Participants quickly agreed on the importance of outcome focused legislation over pre-defined mechanisms for privacy and security policy. They recognized that the changing nature of privacy and security could quickly negate previously accepted standards. Any legislation must allow an organization to adapt to new technologies and standards.

The discussion focused primarily on the topic of privacy, rather than security, and to a large extent was dominated by the need to address the privacy issue itself, rather than its role in legislation, as that was deemed a fundamental starting point.

It was noted that numerous standards organizations have released guidelines for best practices for identity system privacy and security. These organizations include the Identity Ecosystem Steering Group (IDESG), National Institute of Standards and Technology (NIST), and the International Standards Organization (ISO). Many organizations currently develop their internal privacy and security programs by mapping to these standards.

Some participants also expressed the view that additional consideration must be given to privacy and security in situations in which the identity of children may be compromised. Participants emphasized that companies collecting data that can be used to identify children must meet certain standards deemed to be sufficient. Additionally, it is important that any privacy policy must be easily understandable to consumers who may have their information jeopardized.

Many participants noted that privacy and security, like many fundamentals of proper system design, must be considered from the beginning of the design process. This can often begin with defining what data must be collected, the purposes for which it will be used, and how it can be protected. Participants pointed to a Secure Development Lifecycle as critical to privacy and security in the modern world. Many participants also agreed that a private initiative to promote privacy and security is increasingly viewed as a competitive advantage in the modern marketplace. As a result, some participants believed that the current non-binding standards surrounding privacy and security were sufficient to provide consumer and business protections. Additional legislative directives might, some suggested, only serve to hinder business and stifle innovation.

The discussion surrounding privacy and security reiterated the importance of focusing on Level 2 identity management-specific law. Specifically, a key question discussed by the participants was

whether privacy requirements specifically applicable to identity systems should be incorporated into Level 2 identity-specific law, or alternatively, whether any identity-specific law should avoid addressing privacy, and instead, defer to applicable Level 1 general privacy law. The latter approach has been adopted by the EU's eIDAS Regulation (which simply requires compliance with privacy law set forth in the EU Data Protection Directive), and the Virginia Identity Management Act, which does not address privacy at all. Support was expressed for this view. All participants agreed, however, that privacy and security were foundational threshold issues given the usage of personal identity information inherent in a wide array of identity transactions.

(d) Business and Technical Standards

Participants next discussed the role in legislation of relevant business and technical standards to foster interoperability in an identity marketplace. They were presented with the following questions to promote their discussion:

- What is the role of IdM business and technical standards in legislation?
- Should legislation adopt, refer to, or incorporate business or technical standards?
- Should compliance with standards be a legal obligation? A safe harbor?
- How should legislation adapt to changing standards?

Participants generally felt that standards should be open, mature, usable, and stable. The openness of standards is particularly important in scenarios where trust is needed. Trust can be enhanced if all organizations can access standards used to promote interoperability in an identity marketplace. Organizations use standards to define what is adequate, not mandatory, to meet a certain level of design. This means that organizations can go above and beyond the standards when properly incentivized by the marketplace.

One particularly salient issue was the tension between standards-based and outcome-oriented approaches to legislation and regulation. Most agreed regulation and legislation prescribing specific technical processes would hinder innovation and ultimately inhibit the success of new legal regimes.
Participants pointed out that it is much more difficult to remove standards from legislation, than it is to put standards into legislation. It was noted that eIDAS recognized the risks associated with over-defining standards in legislation. To address that issue, eIDAS promotes cooperation between member states and technical experts to address changes in technology and standards as they arise. Legislative gridlock is avoided as changes can be made to the referenced standard without adjusting the underlying legislation.

Participants agreed that an over-definition of standards within legislation would hinder innovation in the identity marketplace moving forward. Legislation should therefore be focused on specific outcomes as opposed to specific standard prescriptions.

(e) Participant Obligations and Related Issues

The final discussion topic of the day addressed identity system participant obligations and related issues in an identity marketplace. Participants were presented with the following questions to guide their discussion:

- What identity provider, relying party, and subject obligations should be imposed by law?
- Should legislation address the rights of non-participants?
- What is role of third party certification in legislation?
- What is role of trustmarks and registries in legislation?

It was noted that some limited provisions addressing participant obligations appeared in both eIDAS and the Virginia legislation. In both cases, however, they were relatively limited and minimal in scope. For example, neither provides the extensive set of participant obligation rules set forth in the old Utah PKI-based legislation. Whether the standards to be adopted in Virginia provide much more detail regarding participant obligations remains to be seen. However, each role is important given that each party in an identity marketplace relies on or provides a verified identity.

Participants agreed that third party rights should be addressed given the personal nature of identity transactions. Regarding third-party certification, some participants promoted the theme of "trust, but verify," meaning that trust should be grounded on meaningful; verification of compliance with given rules and/or standards. It was also noted that legislation can best promote this theme by focusing on outcomes over specific prescriptions.

Finally, participants recognized the challenges that would be faced in any legislative movement in Congress. Many expressed optimism that expert testimony and a united base of agreed upon concepts could persuade policy makers to expedite the process of identity management-specific law. Additionally, efforts by the Uniform Law Commission could be assisted with a common set of important issues to all members of an identity ecosystem.

4. Conclusion

This brief Report seeks to convey some of the key themes and considerations discussed at the meeting. While many topics were touched on only briefly in the limited time available, there did seem to be general agreement that any Level 2 legislation should be outcome focused and promote innovative identity system practices. Moreover, a consensus developed on the need to develop a common set of issues that must be addressed in any identity management-specific law. And while there was disagreement over how to address many of the various issues discussed, participants recognized the need to focus on policy and law in a manner that allows industry to continue to innovate and unlock data assets while protecting the interests of participants throughout the identity management process.

To that end, many recommended looking at analogous law, such as law governing international payment systems, international consumer banking, or international credit card systems, to leverage the ideas and experience we've built up regarding the law in those areas.

* * *

Throughout 2016, Open Identity Exchange will return to these pivotal issues in a series of International Identity, Law and Policy Workshops. Each workshop will examine these issues through the different lenses of a range of experts and stakeholders in the United States, Europe and Amsterdam on March 24th with support from Verizon and DigIdentity. Each workshop's output will in turn inform discussions at the next. The London Workshop in May will be co-sponsored by the UK Society for Computers & Law with support from Microsoft and the UK Cabinet Office Identity Assurance Program. We will report findings at the Cloud Identity Summit in New Orleans in June and our third annual "Economics of Identity" Conference in London in October.

This White Paper and those to follow reflect OIX's goal to complement the work of public and private sector organizations seeking to address international legislation, policy, regulation and law. OIX members hope to contribute to better laws and regulations so as a result, users, customers and citizens might be better served online, and their privacy and security better protected.

Event Participants

Organization	Name
Buckley Sandler LLP	Margo Tank
Certipath	Jeff Nigriny
Consultant	Debra Diener
Consultant	Donald Thibeau
Deloitte	Shelly Hartsook
Deloitte	Colin Soutar
Digicert	Ben Wilson
Digidentity BV	Marcel Wendt
Dinsmore & Shohl LLP	John Costello
DocuSign, Inc.	Ken Moyle
Entrepreneur	Michael Koenitzer
Fannie Mae	Sheilah Goodman
FIDO Alliance	Brett McDowell
Future Law LLC	Tim Reiniger
GB Group PLC	Amy Garner
HID Global	Kathleen Carroll
Identity Assurance Systems, Inc.	Rick Gill
Identity Assurance Systems, Inc.	Isabel Peters
Identity Economy Holdings	Giles Watkins
IdenTrust	Karen Wendel
IDmachines LLC	Salvatore D'Agostino
International Association of Privacy Professionals	Rita Heimes
Internet Society	Christine Runnegar
Livingston PLLC	Lucy Thomson
Locke Lord LLP	Tom Smedinghoff
Microsoft Corp.	Mike Jones
Microsoft Corp.	Tony Nadalin
Microsoft Corp.	Christian Paquin
MorphoTrust USA	Benjamin Silverstein
NASCIO	Yejin Cooke
National Notary Association	William Anderson
OASIS	Jamie Clark
Omidyar Network	William Fitzpatrick
Omidyar Network	Eshanthi Ranasinghe
Open Identity Exchange	Mike Leszcz
Open Identity Exchange	Don Thibeau
Payment Pathways	Richard O'Brien
Pepper Hamilton LLP	Timothy McTaggart

Ping Identity Corporation	John Bradley
Privo	Denise Tayloe
SAFE-BioPharma Association	Gary Secrest
SecureKey Technologies, Inc.	Judy Keator
SecureKey Technologies, Inc.	Rene McIver
SecureKey Technologies, Inc.	Stu Vaeth
Telos Identity Management Solutions, LLC	Lisa Kimball
The Chertoff Group	Jeremy Grant
The World Bank	Cem Dener
The World Bank	Tina George
The World Bank	Mia Harbitz
The World Bank	James Neumann
The World Bank	Alberto Ninio
The World Bank	Robert Palacios
The World Bank	David Satola
TSCP	Shauna Russell
U.S. Dept of Commerce - NIST	Mike Garcia
U.S. Dept of Commerce - NIST	David Temoshok
U.S. General Services Administration - 18F	Diego Mayer
U.S. State Department	Mike Coffee
U.S. State Department (Former)	Hal Burman
UK Cabinet Office	Adam Cooper
UK Cabinet Office	Julian White
UNCITRAL	Luca Castellani
Uniform Law Commission	Pat Fry
Uniform Law Commission	Henry Gabriel
United States Notary Association	Marc Aronson
US Postal Inspection Service	Clayton Bonnell
Verizon	Bjorn Hjelm
Verizon Enterprise Solutions	Mike Polosky
Virginia Department of Motor Vehicles	Dave Burhop
White House - United States Digital Service	Amy Barker
White House - United States Digital Service	Lucy Brady
White House - United States Digital Service	Ginny Hunt
Yoti Ltd.	Julie Dawson