

INTERNATIONAL IDENTITY LAW AND POLICY WORKSHOP

The World Bank

January 14, 2016



Identity Management Legal Task Force

Background Paper for January 14, 2016 Meeting on International Identity Management Law and Public Policy

Businesses and governments are beginning to recognize the critical importance of online identity management, and as a result we are starting to see a strong push for legislation governing this topic. At least two jurisdictions have recently enacted significant identity management legislation, and in July 2015 two new projects to develop potentially significant legislation for identity management began to move forward.

In light of such interest and activity, this meeting will explore possible approaches to identity management legislation, issues that might be addressed by such legislation, and possible policy approaches with respect to such issues. This memo will serve to provide general background information to facilitate those discussions.

To put current and prospective legislation into perspective, it is helpful to look first at the overall three level legal framework that governs identity systems and identity management transactions.

1. The Three-Level Legal Framework that Governs Identity Systems

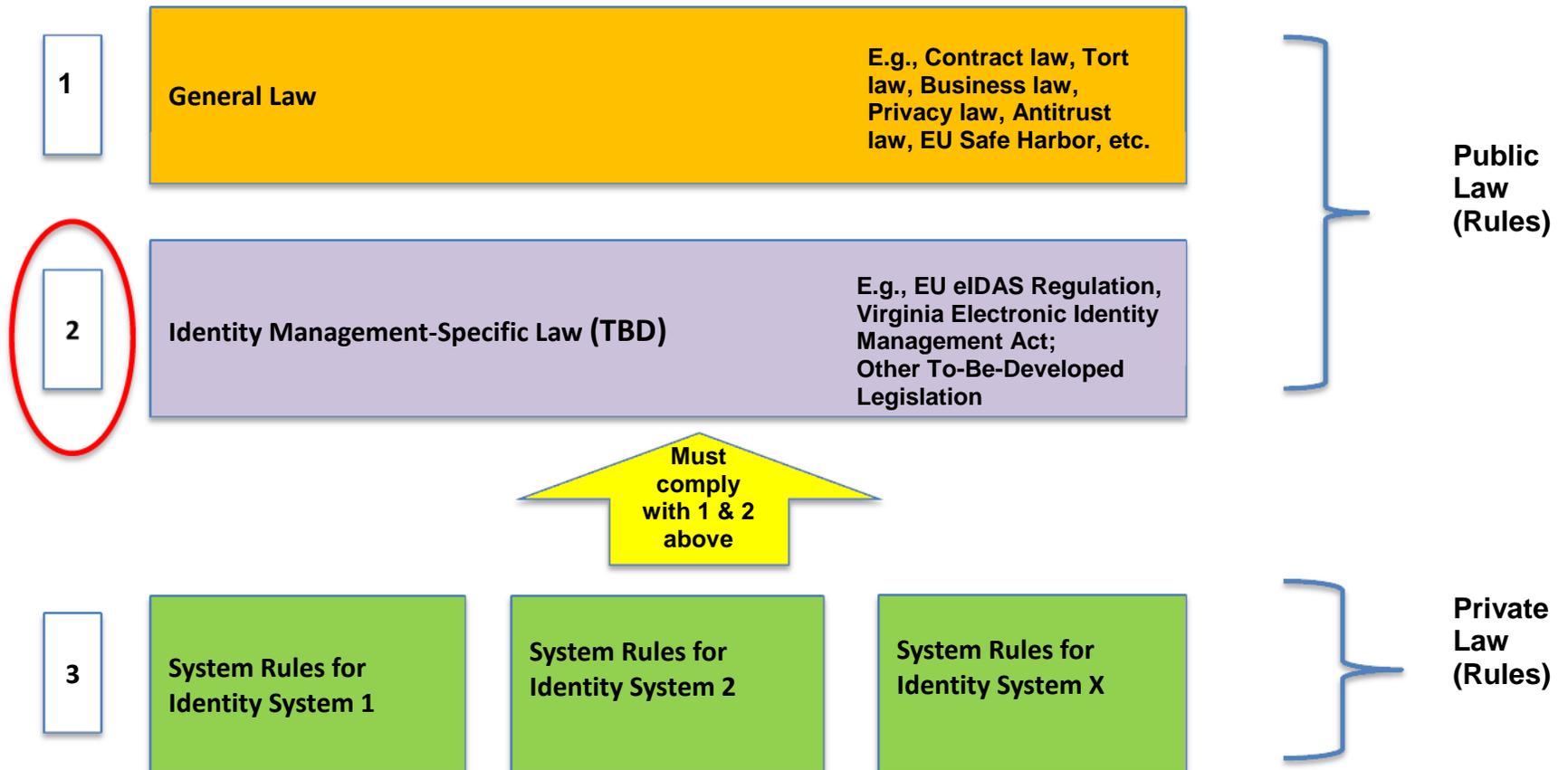
Identity systems, like most commercial multi-party transaction systems, are typically governed by a combination of public law and private law. **Public law** consists of the rules enacted as statutes by legislatures, adopted as regulations by government agencies, or determined by judicial decision. **Private law** consists of contract-based rules drafted by one or more participants or identity system governing bodies.

As depicted in the diagram on the following page, the legal framework in which any identity system operates typically consists of three levels of rules, as follows:

- **(Level 1) General Law:** The first level of applicable rules is general existing law. That is public law that was not written for identity systems, but that is frequently applicable to identity system activities. This includes general contract law, tort law, privacy law, export control law, warranty law, consumer protection law, antitrust law, and the like.
- **(Level 2) Identity Management-Specific Law:** The second level of governing rules consists of identity management-specific law. Very little such public law exists, but it is currently being developed in several jurisdictions. Prime examples are the Virginia Electronic Identity Management Act and the EU eIDAS Regulation (both discussed below). This level will be the focus of our discussion.
- **(Level 3) Individual Identity System Rules:** The third level of rules governing identity systems is the set of contract-based system-specific rules adopted by a particular identity system to govern its own environment. These system rules¹ can be quite detailed, but must comply with the public law rules in Level 1 and in Level 2. The rules at level 3 are private law, and apply within the confines of the identity system they were written to govern, and only to those who have contractually agreed to be bound to them.

¹ System rules are referred to by many different names. These include, for example, “Trust Framework” (used by the U.S. government’s Connect.gov program), “Operating Rules” (used by IdenTrust), “Common Operating Rules” (used by TSCP), “Operating Policies” (used by SAFE-BioPharma) and “Scheme Rules” (used by the UK government’s Gov.UK Verify program). For purposes of this memo, the term “system rules” is used to describe such rules.

Three Levels of Rules Governing Identity Systems



As this diagram illustrates, portions of the legal framework for any identity system (i.e., the Level 3 system rules portion) are under the control of the developers of each specific identity system. That is, the operators of an identity system are free to make up the Level 3 system rules (so long, of course, as the participants agree to be bound by them). But at the same time, the private contracts that make these system rules binding on the participants are subject to and supplemented by (and in some cases overruled by), the existing public law at Levels 1 and 2.

This identity system legal framework is analogous to the legal framework that governs most multi-party transaction systems, such as credit card systems (e.g., Visa, MasterCard, Amex, and Discover), and electronic fund transfer systems (e.g., SWIFT and ACH). For example, each credit card system is governed by Level 3 contract-based system rules (e.g., the Visa Operating Regulations) that specify both: (1) the technical, business, and operational processes and specifications for the credit card system, and (2) the contractually-defined legal rules governing the duties of and relationships between the various parties. The applicable portions of those system rules are made binding on the parties by virtue of a system of contracts.

But those credit card system rules and the associated contracts are also governed by: (1) Level 1 jurisdiction-specific general laws and regulations (e.g., the law of contracts, the law of negligence, law of fraud, and antitrust law), and (2) Level 2 laws and regulations written specifically to regulate credit card systems (e.g., Regulation Z in the U.S.). This combination of Level 3 private system rules and contracts, and Level 1 and 2 public laws and regulations forms the legal framework in which each credit card system operates.

The same kind of legal framework also governs identity systems, although in most cases, no rules currently exist at Level 2. This is our focus. Since efforts are underway to develop and enact identity management-specific legal rules at Level 2, we need to consider what such Level 2 legislation should look like, what it should cover, and how it should address applicable issues.

2. Recently Enacted Level 2 Identity Management Legislation

As a starting point for any consideration of future legislation, it is useful to look at the recently enacted identity management-specific legislation at Level 2. Two such laws currently exist – in the EU and Virginia.

(a) eIDAS

The EU took the lead in legislatively addressing federated identity systems and transactions, beginning with the July 2014 adoption of its eIDAS Regulation². The EU eIDAS Regulation focuses on identity systems that issue credentials for use in online transactions with public sector bodies. Its key goal is mutual recognition of such credentials in cross-border public sector transactions – i.e., to enable individuals who have a digital identity credential issued in one EU

² Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, (referred to as the “eIDAS Regulation” – electronic identification and signature), available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG. See Articles 1-12.

member state to use that same credential to access online public services in another member state.

To achieve that goal, each member state can “notify” the EU Commission of those of its identity systems whose credentials are accepted for its own online public services, and which it feels should be granted mutual recognition by government agencies in other EU member states. Once such notification is made, other EU member states are obligated to accept credentials from those systems for accessing online public services.

The eIDAS Regulation addresses a variety of issues of importance for such “notified” identity systems. These include:

- Eligibility of countries and systems to participate;
- Mutual recognition of identity credentials issued by participating countries;
- Levels of assurance (including minimum technical specifications, standards, and procedures for such levels of assurance);
- Obligations in the event of a security breach;
- Liability of participating member states, identity providers, and parties operating authentication procedures;
- Cooperation of member states and interoperability of their respective identity systems.

In the past year, four Implementing Acts or Implementing Decisions have also been issued under the eIDAS Regulation to address:

- The procedural arrangements for cooperation between member states;³
- The framework for interoperability of member state identity systems;⁴
- Minimum technical specifications and procedures for each of the assurance levels;⁵ and
- Procedures for notification by member states to the Commission.⁶

³ Commission Implementing Decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market; available at <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015D0296&from=EN>.

⁴ Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market; available at <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R1501&from=EN>.

⁵ Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market; available at <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R1502&from=EN>.

⁶ Commission Implementing Decision (EU) 2015/1984 of 3 November 2015 defining the circumstances, formats and procedures of notification pursuant to Article 9(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015D1984&from=EN>

The eIDAS Regulation does not require that a member state’s notified identity systems be government operated. Accordingly, credentials issued by the member state, under a mandate from the member state, or independently of the member state (e.g., by the private sector) but recognized by the member state, are all acceptable. However, they must also comply with the applicable technical specifications, standards and procedures regarding assurance levels set out in the Implementing Acts. And the Regulation holds member states and identity providers liable for damage caused by a negligent failure to comply with its obligations under the Regulation.

(b) Virginia

Shortly after the EU eIDAS Regulation was adopted, the Commonwealth of Virginia became the first U.S. state to enact its own Electronic Identity Management Act.² That legislation took effect on July 1, 2015. It provides for the creation of a Virginia Identity Management Standards Council, which is tasked with developing Identity Management Standards. Once those standards are officially approved by the state, the statute grants immunity from civil liability to trust framework operators and identity providers so long as they comply with the requirements of the Identity Management Standards and the applicable system rules. It also provides for the regulation of identity management trustmarks designed to evidence trustworthy systems.

The issues addressed by the Virginia legislation include:

- The adoption of technical and data standards regarding the verification and authentication of identity;
- The adoption of minimum specifications and standards that should be included in an identity trust framework;
- Liability of identity providers and trust framework providers;
- Trustmarks;
- Warranties created by the use of a Trustmark;
- Satisfaction of commercially reasonable security procedures for electronic fund transfers.

3. Projects to Develop New Level 2 Identity Management Legislation

New efforts to develop public law Level 2 identity management legislation or regulation are now moving forward. The following upcoming projects are worthy of note:

(a) UNCITRAL (United Nations)

The first project to be approved will be an international effort undertaken by the United Nations – specifically by the United Nations Commission on International Trade Law (“UNCITRAL”).

UNCITRAL was established by the United Nations General Assembly in 1966 with a mandate to further the harmonization and modernization of the law of international trade. It does

² Virginia Electronic Identity Management Act (<https://lis.virginia.gov/cgi-bin/legp604.exe?151+ful+CHAP0483>), VA Code §§ 2.2-436 – 2.2-437 at <http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/>, and VA Code §§ 59.1-550 – 59.1-555, at <http://law.lis.virginia.gov/vacode/title59.1/chapter50/>.

this by preparing and promoting the use and adoption of legislative and non-legislative instruments in a number of key areas of commercial law. Those areas include international contract practices, transport, insolvency, electronic commerce, international payments, secured transactions, procurement, sale of goods, and dispute resolution. The legal instruments developed by UNCITRAL are negotiated through an international process involving a variety of participants, including member States of UNCITRAL, nonmember States, and invited intergovernmental and non-governmental organizations. As a result of this process, these texts are widely accepted as offering solutions appropriate to different legal traditions and to countries at different stages of economic development. In the years since its establishment, UNCITRAL has been recognized as the core legal body of the United Nations system in the field of international trade law

In the area of electronic commerce, UNCITRAL's most successful projects include the Model Law on Electronic Commerce (1996), and the UN Convention on the Use of Electronic Communications in International Contracts (2005). In particular, legislation based on or influenced by the Model Law on Electronic Commerce has been adopted in 64 countries (including the U.S.) in a total of 139 jurisdictions (including almost all U.S. states).

2015 Proposal. In the Spring of 2015 the countries of Austria, Belgium, France, Italy, and Poland (with support from the EU Commission), along with the American Bar Association Identity Management Legal Task Force, submitted a proposal to UNCITRAL recommending that it undertake a project to develop "a basic legal framework covering identity management transactions, including appropriate provisions designed to facilitate international cross-border interoperability."⁸ At its July 2015 meeting, UNCITRAL agreed to move forward with such a project. It is expected to formally start in 2016.

As we saw with its prior work in the area of electronic commerce, UNCITRAL provides an international forum capable of developing a harmonized set of globally accepted rules governing identity management. Such rules can be adapted domestically by countries to promote a universal approach to identity management law, and can also be extended globally (to facilitate cross-border identity transactions) through an international convention.

(b) Uniform Law Commission (U.S.)

A second project has been proposed for the development of domestic identity management law in the United States. That project was proposed to, and is currently under consideration by, the Uniform Law Commission.

The Uniform Law Commission ("ULC"), previously known as the National Conference of Commissioners on Uniform State Laws (NCCUSL), was established in 1892. Its goal is to provide states with non-partisan, well-conceived and well-drafted legislation that brings clarity and stability to critical areas of state statutory law. ULC members are practicing lawyers, judges, legislators, and law professors, who have been appointed by state governments to research, draft,

⁸ That Proposal is set out in Document A/CN.9/854 – "Possible future work in the area of electronic commerce - legal issues related to identity management and trust services" available at <http://www.uncitral.org/uncitral/en/commission/sessions/48th.html>

and promote enactment of uniform state laws in areas of state law where uniformity is desirable and practical. Some of the most successful ULC projects include drafting of the Uniform Commercial Code (enacted in all 50 states), and drafting of the Uniform Electronic Transactions Act (so far enacted in 47 states).

2015 Proposal. In June, 2015, a proposal was submitted to the ULC by one of the Commissioners to convene a Study Committee to consider the development of a Uniform Act on Identity Management in Electronic Commerce. The ULC is expected to act on that proposal sometime before spring 2016. If it moves forward with the appointment of a drafting committee, a project to develop uniform identity management legislation for the 50 US states will likely be proceeding in parallel with the project undertaken by UNCITRAL.

(c) Identity Management Standards Advisory Council (Virginia)

One of the provisions of the Virginia Electronic Identity Management Act established the Identity Management Standards Advisory Council (IMSAC) to advise the Virginia Secretary of Technology on the adoption of identity management standards and the creation of guidance documents that will be adopted as regulations in Virginia.

Specifically, IMSAC recommends to the Secretary of Technology guidance documents relating to (i) nationally recognized technical and data standards regarding the verification and authentication of identity in digital and online transactions; (ii) the minimum specifications and standards that should be included in an identity trust framework, so as to warrant liability protection pursuant to the Virginia statute; and (iii) any other related data standards or specifications concerning reliance by third parties on identity credentials.

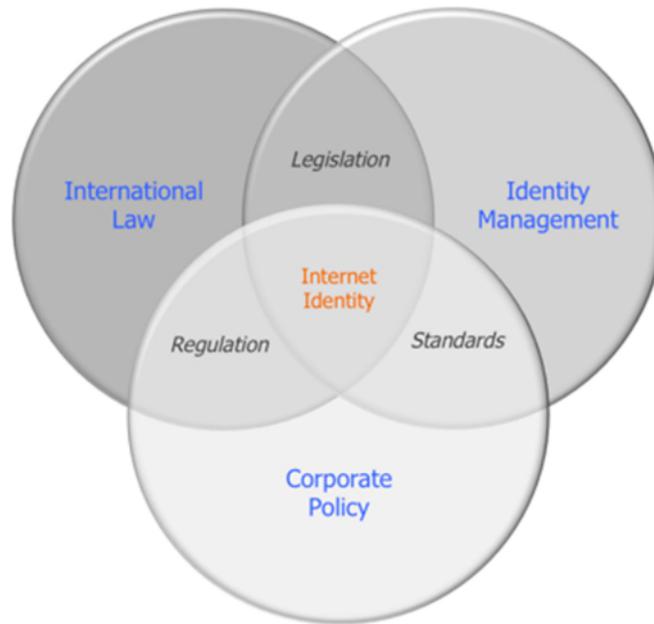
The role of IMSAC is important, as the regulations that result from its deliberations will, in part, determine the imposition of liability on identity providers and trust framework providers subject to the Virginia law.

The eight members of the IMSAC were appointed by the Governor of Virginia on October 5, 2015. IMSAC held its first meeting on December 7, 2015.²

4. Level 2 Legislative Issues

Key questions for each of these legislative or regulatory efforts include what approach such legislation should take to the issue of identity management, what issues it should address (and what issues should it avoid), and what policy positions it should take with respect to the issues it does cover. How should legislative or regulatory efforts attempt to address the issues resulting from the cross-section of International Law, Identity Management, and Corporate Policy as shown in the Venn diagram below?

² <http://vita.virginia.gov/About/default.aspx?id=6442474173>



The following is a brief review of some of those issues, which we would like to discuss in much more detail at the meeting on the 14th.

(a) Trust, Interoperability, Acceptability, and Enforceability

Trust is one of the key issues and challenges facing participants in a federated identity systems. Is the information that I am receiving trustworthy? Can I rely on it? How can I verify its reliability? Etc.

Many approaches have been recommended to enhance trust, including certification that participants comply with required standards, definition of levels of assurance, and other requirements. A key question is how can laws create (or enhance) trust?

The EU eIDAS Regulation addresses trust through the use of levels of assurance and the imposition of minimum technical specifications and procedures. The Virginia Act will presumably address trust through the standards that it adopts, although the approach that it takes remains to be seen.

Related to trust our issues of acceptability, enforceability, and interoperability. Will identity verifications be acceptable and legally enforceable under applicable regulatory schemes or legal requirements?

The EU eIDAS Regulation addresses interoperability, acceptability and enforceability by imposing a duty of mutual recognition (in limited cases), and by establishing an interoperability framework. The Virginia Act may address these issues through the standards that it adopts, although the approach that it takes remains to be seen.

(b) Liability

Fear of liability is one of the most significant legal impediments to participation in the emerging identity market. Recognizing that problems may occur, “What’s my liability?” is one of the questions most commonly asked by organizations considering participating in a multi-party identity system. All parties have concerns. For example:

- Identity providers (IdPs) worry that some of the credentials they issue may be incorrect, and that reliance on that incorrect data may result in significant damages to the relying party, for which they might be held liable;
- Attribute providers (APs) worry that use by IdPs or relying parties of the information they provide might violate the regulatory restrictions applicable to it, exposing them to risk of fines and penalties;
- Relying parties (RPs) worry that their reliance on incorrect identity data might result in significant losses due to fraud and/or render them liable to individuals whose identity may have been stolen; and
- Individuals (data subjects) worry about their liability if someone else misuses their identity credential.

Issues of liability arise whenever someone suffers a loss, be it a financial loss, property damage, or personal injury. The default rule is that any party suffering a loss must bear that loss itself. In many cases, however, there is a legal rule (e.g., a law or a contractual provision) that shifts responsibility for such losses from the party that incurs them to another party – i.e., there is a rule that makes a second party “liable” for the losses of the first party.

All participants must recognize that where a loss occurs, liability is a zero-sum game. That is, if one participant is able to avoid responsibility for damages that flow from a malfunction of the system or failure of performance (such as through a contractual limitation of warranties or disclaimer of liability), the damages do not disappear. Instead, they must be borne by one or more of the other participants. Thus, from a legal perspective, the liability issue is one of allocating responsibility for losses, not eliminating them per se.

The EU addresses the liability issue directly in the eIDAS Regulation. It holds member states liable for damage caused intentionally or negligently due to a failure to comply with its obligations to satisfy the requirements of the technical specifications, standards and procedures set forth in the implementing acts, or to ensure the availability of online authentication. It provides similar allocations of liability for parties issuing identity credentials and operating authentication procedures.

The Virginia legislation specifically allocates liability among the parties with respect to certain issues in identity transactions, based on compliance or non-compliance with the standards to be adopted by the IMSAC. It remains to be seen whether such allocation of liability will promote or hinder the further development of identity systems in the US.

With respect to the issue of liability, the Virginia Act states that an identity provider 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; and
- For noncompliance with any contract or identity trust framework

Conversely, the Virginia Act also states that an identity provider 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; or
- For misuse of any identity credential by any person

(c) Privacy and Security

Any form of identity and attribute management applied to human subjects involves the collection and verification of personal information about an individual. The use and storage of that information by an identity provider, and the potential disclosure of some of that personal information (or information derived from it) to a relying party and other third parties, raises significant privacy and security issues. Thus, by its nature, identity management presents a new challenge to privacy, in that transfers of personal information routinely occur between organizations as well as between the individual and an organization, and may frequently cross industry sectors and jurisdictional boundaries in the process. The more valuable the personal information for informing the relying party’s identity decision, the potentially more intrusive the potential use of that information for individual subjects.

Personal data is a key component of identity transactions and thus, the protection of the privacy and security of such personal data becomes an important consideration. Because the EU is governed by comprehensive privacy law in the form of the Data Protection Directive, the EU approach to protecting the privacy of personal data in identity system transactions is quite simple and straightforward. The eIDAS Regulation simply requires that the processing of personal data be carried out in accordance with the EU Data Protection Directive.

Presumably adopting a similar approach (i.e., comply with existing privacy law) the Virginia Act does not even mention privacy at all, although it is conceivable that privacy and security could be addressed in the standards to be adopted in Virginia..

(d) Business and Technical Standards

Identity system rules (Level 3) generally require compliance with numerous business and technical standards both to ensure that the system works properly, and to ensure that the results are trustworthy. Should any such standards be legally mandated through identity management legislation or regulation? Or should it be left to each individual identity system to determine the standards applicable to its transactions? If so, which standards, etc.?

The EU eIDAS regulation requires compliance with minimum technical specifications, standards, and procedures set out in an implementing act. Conversely, the Virginia Act does not

strictly require compliance with business and technical standards, but rather, provides that compliance with yet-to-be-determined standards specified by the state of Virginia is a safe harbor from liability.

(e) Participant Obligations

The subject of participant obligations is not extensively covered in current identity management legislation. The Virginia statute merely requires that identity providers comply with the Virginia identity management standards as a condition of obtaining the safe harbor from liability, although such standards could presumably address participant obligations in detail. The eIDAS Regulation does go further, however, and requires compliance with assurance levels, imposes requirements regarding uniqueness and correctness of the attribution, imposes an obligation to ensure the availability of authentication online, requires compliance with the implementing act addressing the interoperability framework, and requires compliance with the minimum technical specifications, standards, and present procedures set out in the implementing act governing those issues.

(f) Legislative Goals and Approaches

There are many possible goals for identity management legislation. Some of the more common possibilities include the following:

- Remove barriers to IdM
- Regulate conduct of identity system participants
- Ensure trust of identity credentials
- Incentivize/encourage/promote the IdM marketplace
- Facilitate cross-border interoperability of IdM transactions
- Protect participants in identity transactions (e.g., consumers)
- Ensure the acceptability and/or enforceability of identification/authentication
- Technology neutrality
- Interoperability (of ID systems within a country; and of one country's system with another's)
- Cross-border recognition