United Nations

A/CN.9/WG.IV/WP.120

General Assembly

Distr.: Limited
27 July 2012

Original: English

United Nations Commission on International Trade Law
Working Group IV (Electronic Commerce)
Forty-sixth session
Vienna, 29 October-2 November 2012

Overview of identity management

Background paper submitted by the Identity Management Legal Task Force of the American Bar Association

Note by the Secretariat

Within the framework of preparation for the forty-sixth session of Working Group IV (Electronic Commerce), the Identity Management Legal Task Force of the American Bar Association submitted the attached document to the Secretariat.

The document in the attached annex is reproduced in the form in which it was received by the Secretariat.

I. Introduction

1. In 2011, an OECD report noted that “digital identity management is fundamental to the further development of the Internet economy.”[1] It is a foundational requirement for all substantive forms of e-commerce.

2. This paper provides an overview of identity management, its role in e-commerce, the legal issues it raises and the legal barriers it presents.[2] It is based on the ongoing work of the Identity Management Legal Task Force of the American Bar Association (ABA),[3] and is submitted as background to inform the Working Group of relevant issues.[4]

3. At its forty-fourth session, in 2011, the Commission agreed that Working Group IV (Electronic Commerce) should be convened to undertake work in the field of electronic transferable records.[5] At the same time, the Commission agreed that the extension of the Working Group’s mandate to other topics discussed in document A/CN.9/728 and Add.1 as discrete subjects (as opposed to their incidental relation to electronic transferable records) would be further considered at a future session.[6] Those topics included identity management, single window, and mobile payments.[7]

4. As discussed below (paras. 6-7), identity management is a fundamental requirement for each of the topics considered by the Commission at its forty-fourth session (electronic transferable records, single window, and mobile payments). Thus it will be important for the current work of the Working Group on electronic transferable records, as well as for any possible future work on the other topics.

[1] OECD (2011) “Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy — Guidance for Government Policy Makers,” *OECD Digital Economy Papers*, No. 196, OECD Publishing, at p. 3; available at www.oecd-ilibrary.org/science-and-technology/digital-identity-management-for-natural-persons_5kg1zqsm3pns-en.

[2] This paper focuses on commercial identity management systems intended for use in a business context, including business-to-business (B2B), business-to-government (B2G), and business-to-consumer (B2C) communications.

[3] Identity Management Legal Task Force, Cyberspace Law Committee, American Bar Association, Section of Business Law; http://apps.americanbar.org/dch/committee.cfm?com=CL320041. The views expressed in this paper have not been approved by the House of Delegates or the Board of Governors of the American Bar Association and, accordingly, should not be construed as representing the policy of the ABA.

[4] Additional materials are also available from the proceedings of the UNCITRAL Colloquium on E-Commerce, 14-16 February 2011 New York at www.uncitral.org/uncitral/en/commission/colloquia/electronic-commerce-2010.html.

[5] *Official Records of the General Assembly, Sixty-sixth Session, Supplement No. 17* (A/66/17), para. 250.

[6] Ibid., para. 251.

[7] Ibid., paras. 241-49.

5. The critical importance of identity management in facilitating trustworthy e-commerce is well-recognized. Numerous intergovernmental groups, states, private international groups, and commercial entities are actively exploring identity management issues and opportunities, developing technical standards and business processes, and seeking ways to implement viable identity systems. For example:

(a) Inter-governmental groups actively working on identity management issues and standards include the Organization for Economic Cooperation and Development (OECD),[8] the International Organization for Standardization (ISO)[9] and the International Telecommunications Union (ITU);[10]

(b) A survey undertaken by the OECD[11] identified 18 OECD countries actively pursuing national strategies for identity management (Australia, Austria, Canada, Chile, Denmark, Germany, Italy, Japan, Luxembourg, Netherlands, New Zealand, Portugal, Republic of Korea, Slovenia, Spain, Sweden, Turkey, and United States of America).[12] Several other countries, such as Estonia, India, and Nigeria are also actively pursuing such strategies;

(c) Several regional identity projects are underway in the European Union, including PrimeLife (a project of the European Commission's Seventh Framework Programme),[13] the Global Identity Networking of Individuals — Support Action (GINI-SA),[14] STORK (to establish a European eID Interoperability Platform),[15] and the European Network and Information Security Agency (ENISA);[16]

(d) Private organizations working on identity standards and policy at an international level include the Organization for the Advancement of Structured Information Standards (OASIS),[17] the Open Identity Exchange (OIX),[18] the Kantara Initiative,[19] the Open ID Foundation,[20] tScheme,[21] and The Internet Society;[22]

(e) Some commercial identity systems have been established and operate on a global scale in limited areas. These include those operated by the Transglobal Secure Collaboration Program (TSCP)[23] and CertiPath[24] for the aerospace and defence industries, the SAFE-BioPharma Association[25] for the biopharmaceutical

[8] www.oecd.org/document/38/0,3746,en_2649_34255_49319782_1_1_1_1,00.html.

[9] www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=45306.

[10] www.itu.int/ITU-T/studygroups/com17/fgidm.

[11] Bernat, L. (2011), "National Strategies and Policies for Digital Identity Management in OECD Countries", OECD Digital Economy Papers, No. 177, OECD Publishing. doi: 10.1787/5kgdzvn5rfs2-en; at www.oecd-ilibrary.org/content/workingpaper/5kgdzvn5rfs2-en.

[12] Ibid., at pp. 28-35 for a list of links to national documents.

[13] www.primelife.eu.

[14] www.gini-sa.eu.

[15] https://www.eid-stork.eu.

[16] www.enisa.europa.eu.

[17] www.oasis-open.org/home/index.php.

[18] www.openidentityexchange.com.

[19] http://kantarainitiative.org, formerly known as the Liberty Alliance, www.projectliberty.org.

[20] http://openid.net/foundation.

[21] www.tscheme.org.

[22] www.internetsociety.org.

[23] www.tscp.org.

[24] https://www.certipath.com.

[25] www.safe-biopharma.org.

industry, IdenTrust[26] for the financial sector, the CA/Browser Forum[27] for website EV-SSL certificates, and FiXs — Federation for Identity and Cross-Credentialing Systems (FiXs).[28] The work of these groups is focused primarily on technical standards and business process issues, rather than legal issues.

II. How does identity management relate to e-commerce?

6. Identity management is a foundational issue for most e-commerce transactions and other online activities. Verifying the identity of remote parties, such as determining who is seeking access to an online database of sensitive information, who is trying to do an online transfer of funds from an account, who signed an electronic contract, who remotely authorized a shipment of product, or who sent an email, is a fundamental concern. While participants in many low-risk online transactions are willing to trust that they are dealing with a specific person or entity, as the sensitivity or value of the transaction increases, the importance of ensuring the availability and reliability of accurate information about the identity of the remote party in order to make a trust-based decision increases as well.

7. Identity management is a basic requirement for electronic signatures, for the topic of electronic transferable records, and for any possible future work on the other topics (single window and mobile payments).[29]

(a) Establishing identity of the signer is one of the requirements for creating a valid electronic signature. Both Article 7 of the UNCITRAL Model Law on Electronic Commerce (1996) and Article 9 of the United Nations Convention on the Use of Electronic Communications in International Contracts (2005, Electronic Communication Convention) require, as a condition of a valid electronic signature, that a “method is used to identify” the signer that is as reliable as was appropriate for the purpose for which the data message was generated or communicated. Article 2 of the UNCITRAL Model Law on Electronic Signatures also requires data “which may be used to identify the signatory” as a component of an electronic signature;

(b) Verification of identity is also a critical requirement for electronic transferable records, single window, and mobile payments. Current law regarding electronic transferable records requires establishing the identity of both the signer of the record as well as the holder entitled to enforce it.[30] Single window processes will require establishing the identity of the signer of customs documents, as well as the identity of the person or entity filing them and the person or entity entitled to enforce them.[31] And mobile payments, like all other payment systems, require (for purposes of authorization) the identity of the person purporting to transfer funds.[32]

[26] www.identrust.com.

[27] www.cabforum.org.

[28] www.fixs.org.

[29] *Official Records of the General Assembly, Sixty-sixth Session, Supplement No. 17* (A/66/17), paras. 241-252.

[30] A/CN.9/WG.IV/WP.115, paras. 24-26 and 45-48.

[31] A/CN.9/728/Add.1, paras. 42 and 45.

[32] See, A/CN.9/728, para. 52.

III. What is identity management?

8. At its essence, identity management is designed to provide the answer to two simple questions that each party to an online transaction asks about the other party: "Who are you?" and "How can you prove it?" The ability to provide a reliable and trustworthy answer to these questions is fast becoming a critical requirement for electronic business activities, especially as the nature, significance, and sensitivity of those transactions increases. With the answers to those two questions, a party to an online transaction can decide whether or not to engage in the transaction (e.g., whether to enter into a contract with the other party, whether to allow the other party to access a sensitive database, or whether to extend some other privilege or access to the other party).

9. Every entity that engages in digital transactions could set up its own system to identify and authenticate each of its business partners (as many businesses currently do through the use of individual registration processes coupled with a username and password system), but this is increasingly proving expensive and inadequate, producing challenges to scaling the system to broader populations. Moreover, the increasing need for cross-organization collaboration, concerns about security, and the problem of user password management suggest that the traditional company-issued or vendor-issued username and password approach is no longer adequate.

10. As a consequence, identity systems whereby a third party identity provider (or attribute provider) plays a key role are emerging as a preferred approach. The goal is to allow businesses and government agencies to conduct electronic transactions with remote parties in reliance on identity information and authentication processes provided by any one of several unrelated third party providers. This is often referred to as a "federated" identity system. In other words, identity information verified by one entity is made available in an agreed-upon and managed fashion to multiple parties across different systems that have a need for identity information for various purposes. This would, for example, allow individuals and businesses to use an identity credential of their choosing to conduct online transactions with numerous enterprises, just as an individual might use a driver's licence for a variety of different offline transactions with different entities, such as buying alcohol, gaining admission to an airport boarding area, or opening a bank account.

11. To develop a federated identity system requires a combination of technical standards and systems,[33] business processes and procedures, and legal rules that, taken together, establish a trustworthy system for: (i) verifying identity and connecting that identity to an individual human, legal entity, device, or digital object, (ii) providing that identity information to a party that requires it to authorize a transaction, and (iii) maintaining and protecting that information over its life cycle. Critical to making it work in a commercial context is the requirement for an appropriate, and typically contract-based legal framework that defines the rights and responsibilities of the parties, allocates risk, and provides a basis for enforcement. This legal framework is often referred to as "operating rules" or a "trust framework"

[33] A public-key infrastructure (PKI) is one approach that can be used to build an identity system. However, many other technologies and approaches are also being developed, and implemented.

IV. Identity management basics

12. Although the term "identity management" is relatively new, the concept is not. The underlying processes have long been in use in an offline environment. Passports, driver's licences, and employee ID cards are all components of identity systems (i.e., they are credentials issued by an entity to verified individuals so those individuals can later validate their identity). The process of identifying a person and issuing the credential can be done by the party that also accepts the credential (as in the case of a company-issued employee ID card), or by a third party (as in the case of a driver's licence or passport). A key element of federated systems, where there is a third party issuer, is that the use of these identity credentials is not limited to transactions with the entities that issued them. Rather, they are designed and deployed with the anticipation that the credentials will be accepted by third parties (such as airport security, a bank, or a bartender in the case of a driver's licence) when proof of certain attributes of one's identity (e.g., name or age) is required.

13. The challenge is to implement a similar capability in an online environment. That is, to create a system for secure, reliable and trustworthy digital identity credentials that can be used remotely across different systems and entities (i.e., to develop a federated identity system). This allows data subjects to use the same identity credential to identify themselves in order to access resources or conduct transactions with multiple organizations.

14. While there are many different approaches to identity management, it essentially involves two fundamental processes: (i) the process of collecting and verifying certain identity attributes about a person (or entity, device, or digital object)[34] and issuing an identity credential to reflect those attributes ("identification"), and (ii) the process of later verifying that a particular person presenting that credential and claiming to be that previously identified person is, in fact, such person ("authentication"). Each of these basic processes can involve various sub-processes, depending on the nature of the data and context in which the two processes take place. Once identity attributes about an individual are successfully authenticated, a third set of processes, referred to as "authorization," is engaged in by the entity that intends to rely on the authenticated identity to determine what rights and privileges are accorded to such person (e.g., whether to enter into a contract with such person, or whether such person should be granted access to a database, an online bank account).

A. Identification

15. The identification process is designed to answer the question "who are you?" Performed by someone filling the role of an identity provider[35] it involves associating identifying attributes (such as name, membership number, address, or birth date) with a person in order to identify and define that individual to the level

[34] Identity information can be collected and verified, and identity credentials can be issued, for individuals, legal entities, devices, and digital objects. This paper focuses only on identity systems with respect to individuals.

[35] In some case, where only selected attributes are required for the identification process, an entity known as an attribute provider fills this role.

sufficient for the contemplated purpose. Sometimes called “identity proofing” or “enrolment,” this process is often a one-time event. It typically involves the collection by an identity provider of information about the person to be identified (referred to as the “subject”), and often relies on a patchwork of government-issued documents (e.g., a birth certificate, social security card, driver’s licence, and passport), as well as credentials issued by private sector entities (e.g., an employee badge, mobile wireless SIM card, and credit cards). Although such identity documents and credentials were issued for other purposes, they can often be re-used to facilitate later identification processes in new contexts. This occurs, for example, when someone provides a driver’s licence to prove their identity in the context of receiving an employee identity badge.

16. At the end of the identification process, the subject’s relevant identity attributes are typically represented by data in an electronic document issued by the identity provider and referred to as an identity credential. A credential presents (or links to or correlates with) data that is used to authenticate the claimed digital identity or attributes of a person, entity, or device.[36] A credential can be embodied in a variety of media. In the physical world, examples of an identity credential include a royal seal, a driver’s licence, a passport, a library card, or an employee identification badge. In the online world the identity credential might be as simple as a user ID, or as complex as a cryptographically-based digital certificate that might be stored on a computer, cell phone, smart card, ATM card, flash drive or similar device.

B. Authentication

17. When a person presents an credential (such as by presenting a driver’s licence at an airport or entering a user ID on a corporate network), claims to be the person identified by the credential, and seeks to exercise a right or privilege granted to such individual (e.g., to board a plane, to access the corporate network or a sensitive database), an authentication process is used by a “relying party” to determine whether that person is, in fact, who they claim to be. In other words, once someone makes a declaration of who they are (by claiming to be the person identified in the identity credential), authentication is designed to answer the question “OK, how can you prove it?” It is a transaction-specific event that involves associating a person with an identity credential to verify that the person trying to engage in the transaction really is the person that was previously identified by the credential.

18. Authentication typically requires something to tie the person to the credential, generally referred to as an authenticator. If the credential is a driver’s licence or passport, the authenticator is the picture and the association is typically done by comparing the picture on the licence or passport to the person presenting it. With electronic credentials, the authenticator is typically something the individual “knows” (e.g. a secret password, or personal identification number), something the individual “possesses” (e.g., a private cryptographic key, a physical device such as a smart card, USB, or other type of token), or something the individual “is,” such as a physical characteristic (e.g., a picture, fingerprint, or other biometric data).

[36] OECD Guidance for Electronic Authentication (2007), at page. 12, available at: http://www.oecd.org/dataoecd/32/45/38921342.pdf.

C. Authorization

19. Once a person is successfully authenticated, the relying party may use its own authorization process to determine what rights and privileges are accorded to such person (e.g., whether such person should be granted access to a website, a database, a bar, or an airport boarding area). This process addresses the question "What can you do?" Thus, authentication of identity is not just an end in itself. It is often used to facilitate the relying party's authorization decisions such as to grant rights or privileges (e.g., to access online system resources), or to enter into a transaction. For example, once the identity of someone seeking access to a computer network has been authenticated, the system owner (i.e., the relying party) may use an authorization process to determine what access rights should be granted to such person. Likewise, once the identity of someone seeking to enter into an electronic transaction (e.g., an electronic contract) has been authenticated, a relying party may use an authorization process to determine whether to proceed with a transaction with the subject or otherwise rely on the communication.

D. Federated identity

20. For online transactions, identification and credential issuance has traditionally been done by the same party that intended to also rely on the credential. For example, a business would identify an employee, and issue him a username and password so he could access the company's network. In that case, the company acts as both the identity provider (since it identified the person as its employee and issued an identity credential) and the relying party (since it also accepts and relies on those identity credentials to grant access to its network).

21. In a "federated" identity system, the functions of the identity provider and relying party not necessarily performed by the same entity. Instead, multiple unrelated relying parties can rely on identity credentials provided by any one of several independent identity providers. Under such a model, a single identity credential can be relied on by numerous organizations that had no direct involvement with the original issuance of the credential.

22. A familiar offline example of a federated identity management process is the way driver's licences are currently issued and used. Issued by a government agency, they are used by various unrelated relying parties to verify attributes about the identity of the subject of the licence. For example, they are used by a security agent to verify the name of a person seeking to enter an airport boarding area, or by a bartender to verify the age of a person ordering a drink.

23. An online example of a federated identity system is the ATM system. In a typical ATM transaction, an individual with an account at Bank A can use the identity credential issued by his bank (the ATM card) to obtain cash from an ATM machine operated by Bank B (with whom he has no relationship). To accommodate the transaction, notwithstanding the absence of such relationship, Bank B contacts Bank A through the ATM network to determine whether the individual is a valid customer of Bank A, to have Bank A authenticate the identity of the individual (i.e., did that person enter the correct password), and to obtain certain identity information about the individual from Bank A (e.g., whether that person's account

has funds sufficient to cover the requested withdrawal, as well as the balance in that person's account so Bank B can print it on the transaction receipt).

IV. Identity system risks

24. There are several potential risks to participating in an identity system and relying on identity data. Those risks include:

(a) Identification risk: The reliability of the identity information collected and asserted about the subjects is critical to the use of any identity system. Identification risk is the risk that identity attribute data collected and associated with a specific subject is inaccurate. This risk is often a function of the quality of off-line identity credentials provided by the subject for identity verification;

(b) Authentication risk: Identification is of no value unless a relying party has the ability to authenticate it (i.e., associate the claimed identity attributes to the correct subject). Authentication risk includes both the risk that a legitimate subject cannot be properly authenticated, as well as the risk that an authentication process will incorrectly indicate that an imposter is a legitimate subject;

(c) Privacy risk: In the case of individuals, identity management involves the collection and verification of personal information about a subject by an identity provider and the sharing of that information with multiple relying parties. In addition, identity-based transactions may also facilitate tracking an individual's activities, thereby generating additional personal information. Privacy risk focuses on the unauthorized use or misuse of personal information about the subject by one of the parties who has access to it, as well as on their compliance obligations with respect to the processing and protection of such data;

(d) Data security risk: Protecting personal information about human subjects, as well as maintaining the security of the processes necessary to create secure identity credentials, communicate accurate identity information, verify the status of identity credentials, and authenticate subjects, is critical to any identity system. Security risk includes the risk that an unauthorized party can obtain access to personal data, as well as the risk of compromise of any of the processes critical to the overall functioning of the identity system or any individual identity transactions;

(e) Liability risk: In any identity system, failures will inevitably occur, and damages will result. Participants in an identity system must address the risk that they will be held liable for damages suffered by someone else resulting from a problem they caused or for which they are deemed legally responsible. A key aspect of the liability risk is the legal uncertainty regarding the responsibility that attaches to any given act or failure to act by a participant in an identity system, particularly one that operates across multiple industry sectors and jurisdictions;

(f) Enforceability risk: Enforceability risk is complementary to liability risk. It is the risk that one participant will not be able to enforce (i) its right to compliance with the rules by another participant, or (ii) its right to collect damages in event it is actually harmed in a case where another participant is legally "liable." This risk applies when something goes wrong and someone seeks to recover damages. It also applies in situations where a problem has not yet surfaced, but a failure of performance on the part of one or more participants can put the entire identity system at risk. This is particularly important in a cross-jurisdictional system. In such case, enforceability risk refers both to the ability to detect that problem, as well as the ability to require the participant to remedy its performance or withdraw from the system;

(g) Regulatory compliance risk: In many cases, participation in an identity system raises legal compliance issues for one or more of the participants (i.e., whether the conduct of the participant complies with applicable local law). In other cases, participation in the identity system is, in and of itself, pursued in an effort to comply with legal requirements imposed on a participant. For example, a financial institution may participate, and rely on identity credentials, in order to satisfy its legal obligations to properly authenticate individuals granted online access to bank accounts and payment facilities. In such cases, compliance risk focuses on whether such participation satisfies it legal obligations.

25. As with any system, the foregoing risks are a function of the technology used, the various processes implemented, and the manner or failure of performance of obligations by the participants themselves (and possible influence by outsiders). Building a reliable identity system will require measures to address these risks, that is, measures designed to ensure that participants can trust the technology used (i.e., that it works properly), the processes deployed (i.e., that they yield the correct result), and other participants (i.e., that they will properly perform their obligations).

V. Addressing functionality and risk: operating rules

26. Making a federated identity system work in an online environment, and addressing the risks such as those noted above, requires not only the implementation of appropriate technology, but also adherence by all participants (e.g., subjects, identity providers, and relying parties) to a common set of technical standards, operational requirements, and legal rules. Commercial identity systems typically seek to achieve that goal by developing appropriate “operating rules” (sometimes referred to as a trust framework) to which participants are contractually bound.

27. Identity system operating rules consist of two general categories of components: (i) the business and technical operational rules and specifications necessary to make the system functional and trustworthy, and (ii) the contract-based legal rules that, in addition to applicable laws and regulations, define the rights and legal obligations of the parties specific to the identity system and facilitate enforcement where necessary.

(a) The business and technical operational rules define the requirements for the proper operation of the identity system, define the roles and operational responsibilities of the participants, and provide adequate assurance regarding the accuracy, integrity, privacy and security of its processes and data (i.e., so that the various parties are willing to participate; so it is trustworthy). In many cases, such rules are built on existing standards;

(b) The contract-based legal rules consist of the contract-based agreements between or among the participants that define and govern the legal rights, responsibilities, and liabilities of the participants with respect to the specific identity system, clarify the legal risks parties assume by participating in the identity system (e.g., warranties, liability for losses, risks to their personal data); and provide remedies in the event of disputes among the parties, including methods of dispute resolution, enforcement mechanisms, termination rights, and measures of damages, penalties and other forms of liability. They also make the business and technical operational rules legally binding on and enforceable against the participants.

28. Both the business and technical operational rules and the contract-based legal rules are, of course, subject to, and typically constructed with reference to, other existing duties and obligations arising under the statutory and regulatory law that apply to the parties. Both components of the identity system operating rules (i.e., both the business and technical operational rules and the legal rules) are subject to the existing statutes and regulations that apply in the jurisdiction(s) where the identity system will operate or be used.

29. Identity system operating rules are much like the operating rules used for credit card systems or electronic payment systems, which must be able to accommodate numerous participants, in a variety of jurisdictions, in accordance with a common rule set. The credit card operating rules, for example, regulate issuers, processors, relying party merchants, and individual cardholders, and provide the specifications and rules applicable to the participants in online credit transactions and subsequent processing.[37] Likewise, electronic funds transfer system operating rules regulate the responsibilities of all of the banks in the payment process, as well as, to a limited extent, the consumers or other payers involved, and provide the specifications and rules applicable to the participants whenever electronic funds transfers (e.g., SWIFT transfers) are used to facilitate payment in an online transaction.[38]

30. Although the need for identity system operating rules containing appropriate legal rules is generally acknowledged, developing them is largely uncharted territory. Numerous legal issues and legal barriers must be identified and addressed.

VI. Law governing identity systems

31. In most jurisdictions, there are numerous existing laws and regulations that will have a significant regulatory impact (and which may impose barriers,

[37] The credit card operating rules includes the credit card issuer specifications and rules (e.g., the Visa International Operating Regulations at http://usa.visa.com/merchants/operations/op_regulations.html and the Payment Card Industry Data Security Standards — PCIDSS at https://www.pcisecuritystandards.org/security_standards/index.php) that are made binding on the processing banks and the merchants, as well as the contracts between the credit card issuers and the processing banks, the contracts between the processing banks and the merchants, and the contracts between the processing banks and the cardholders. And it is supplemented by laws and regulations that govern credit card processing in each relevant jurisdiction.

[38] The electronic funds transfer operating rules includes the specifications and rules for EFT transactions (e.g., the Operating Rules and Guidelines of U.S.-based NACHA — The Electronic Payments Association, http://www.nacha.org/) that are made binding on the processing banks and the merchants, as well as the contracts between the merchants and the individual payers. And it is supplemented by laws and regulations that govern electronic funds transfers, such as (in the U.S.) the Electronic Funds Transfer Act and Regulation E.

compliance requirements, and/or liability risk) on participation in an identity system. In addition, differences among the laws of different jurisdictions, when considered in light of the global nature of the internet, create a patchwork regulatory landscape that can itself challenge legal structuring. Some of these laws and regulations focus specifically on identity-related activities. Most, however, were developed in a context completely unrelated to identity management (e.g., tort law, contract law, and warranty law), but may nonetheless have a significant impact, and often in ways that were unanticipated at the time of their original adoption.

32. Some of the categories of law applicable to identity systems (or participants in them), include the following:

(a) Law governing the accuracy of identity information: Identity system activities focus on the collection and verification by identity providers or attribute providers of information about subjects, and communication of some of that information to relying parties. This often occurs in situations where the accuracy and/or reliability of that information are important. Thus, laws regarding providing false or incorrect information, whether intentionally or negligently, will be relevant in the evaluation of the rights, obligations, and liabilities of the participants in identity systems. Key among those are the tort law governing negligent misrepresentation, negligent endorsement, and defamation, as well as warranty laws, identity theft laws, and laws governing unfair and deceptive business practices;

(b) Law governing the privacy of identity information: By its nature, identity management typically involves the collection (by an identity provider or its agents) and disclosure (to a relying party) of personal information about a subject.[39] Thus, data protection laws, privacy laws, and other laws and regulations governing the collection, use, processing, transfer and storage of the personal data will have a major impact on identity management activities. While many of such laws were written at a time prior to the advent of digital identity systems, and could not therefore have anticipated the particular processes or potential harms involved in such systems, they can nonetheless have a direct impact on such activities;

(c) Law governing the collection of identity information: In addition to privacy and data protection laws, laws governing the re-use of public sector information affect businesses creating information products and services based on bulk data from the public sector. They may create legal barriers to the large-scale use of data maintained by public sector bodies in the context of identity services;[40]

(d) Law governing the security of identity information and processes: Many laws impose obligations on companies with respect to the security of personal information (as variously defined in different jurisdictions, and under the particular laws of a given sector) and other data in their possession. In addition to laws and regulations imposing an obligation to implement security measures to protect data, many jurisdictions have also enacted laws and regulations that impose an obligation to disclose security breaches involving personal information to the persons affected;

[39] Except where the subject is not a human being — e.g., where the subject is a corporation, device, software application, etc.

[40] See generally, Global Networking of Individuals (GINI), Legal provisions for Deploying INDI Services (October 5, 2011) at Section 5, available at www.gini-sa.eu/images/stories/2011.11.06_GINI_D3.1_Legal%20Provisions%20for%20Deploying%20INDI%20Services_FINAL.pdf

(e) Laws focused on a duty to identify: Many laws and regulations require identity as a component element, particularly in an electronic environment. For example, the Electronic Communication Convention expressly requires identity as a component of a legally binding electronic signature. Specifically, where a law requires that a communication or a contract should be signed by a party, the Electronic Communication Convention provides that the signature requirement is satisfied if a method is used to identify the party and to indicate that party's intention in respect of the information contained in the electronic communication;[41]

(f) Laws focused on a duty to authenticate: Several laws regulate one or more elements of authentication. Some impose on businesses a duty to authenticate the persons with whom they deal remotely, and others regulate aspects of the authentication process. One prominent example is the requirements of the U.S. banking regulators for authentication in online banking activities. Specifically, financial institutions offering Internet-based products and services to their customers are required to "use effective methods to authenticate the identity of customers using those products and services."[42] Other countries, such as Singapore, have also adopted similar requirements;[43]

(g) Laws specifically regulating identity system activities: Some jurisdictions have statutes that expressly regulate some aspects of identity management activities. One example is the EU Electronic Signatures Directive,[44] which mandates that member states regulate the collection of personal data about subjects by certain identity providers (called certification service providers), and regulates the issuance of credentials.[45] Similarly, the UNCITRAL Model Law on Electronic Signatures (articles 8-12) sets forth rules for the issuance and use of the identity credentials required for the creation of certain electronic signatures.

H. Challenges and legal barriers

33. Existing laws and regulations of the types noted above, as well as others, pose several basic problems for the development and operation of private sector identity systems. These challenges include the following:

(a) Law not written to address identity management: Many novel issues raised by identity management processes are simply not addressed by existing law. Most existing laws that apply in these contexts were not written from the perspective of digital identity systems, and thus often inadequately or inappropriately address or regulate identity activities. For example, existing law is typically silent with regard to the duty of care an identity proofer must meet when evaluating the authenticity of identity proofing documents, or the scope of any disclosure duty owed by an identity provider to a data subject;

[41] Electronic Communication Convention Article 9(3).

[42] Federal Financial Institutions Examination Council ("FFIEC"), "Authentication in an Internet Banking Environment," October 12, 2005, at p. 1; available at www.ffiec.gov/pdf/authentication_guidance.pdf.

[43] Monetary Authority of Singapore, Circular No. SRD TR 02/2005, 25 November 2005.

[44] Directive 1999/93/EC of 13 December 1999 on a Community Framework for Electronic Signatures ("EU Electronic Signatures Directive"), Articles 6 – 8 and Annexes I and II, available at http://europa.eu/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf.

[45] EU Electronic Signatures Directive, Article 8.

(b) Legal uncertainty/ambiguity: There are some identity management issues that existing laws and regulations may address, but the applicability of those laws is often unclear or ambiguous, leaving identity system participants with a great deal of legal uncertainty that can retard growth, innovation and investment. Thus, even where existing law applies to identity management, the manner in which it will apply to a specific issue or proposed approach in an identity system may not be clear. This is particularly true with respect to laws focused on a specific technology. This may limit the ability of parties entering into identity transactions to assess and manage the risks they assume by so doing;

(c) Privacy issues: By its nature, identity management typically involves the collection by an identity provider and disclosure to a relying party of some personal information about a subject. To participate in an identity system, subjects must disclose personal information, and thus expose themselves to the risk of the unauthorized or inappropriate use of such information. In addition, as subjects interact with multiple relying parties, the required communication or verification of their information by the identity provider allows it to track each subject's activities, giving rise to concerns about the collection and use of such transaction information. Thus, privacy is a key issue for any identity system. This may involve addressing questions such as: (i) What information may be collected by the identity provider?; (ii) How much information may be disclosed to relying parties?; (iii) What control does the subject have regarding disclosure?; (iv) How securely must the data be handled by the parties?; and (v) What limits are imposed on use of the information by the identity provider and relying parties? These questions are often addressed by existing laws, which may also be supplemented by contract-based operating rules;

(d) Liability issues: A legal concern of primary importance to the participants in any identity system is determining who will bear liability associated with any of the risks (see para. 24 above). Numerous statutory, common law, and contract theories have been advanced to identify, define, and clarify the source and scope of such potential liabilities.[46] Yet, these legal risks are often ill-defined and uncertain. The concerns around liability represent a key barrier to private sector adoption of interoperable identity solutions. Addressing liability issues by operating rules or other forms of contractual agreement among the participants is often the best approach, particularly because this permits the contract "customization" needed to address the appropriate risk allocation that will vary from case-to-case;

(e) Jurisdictional variations and conflicts: There are some key issues on which the application of existing laws and regulations to identity activities varies considerably across jurisdictions. This is often the case with respect to laws governing participant liability and data protection laws governing the privacy of personal information. Moreover, in some cases, regulation or licensing of identity system activities may pose additional barriers to the cross-border operation of identity systems. Thus, when identity systems operate across jurisdictional borders, the challenges of developing appropriate operating rules are compounded by the fact that existing laws and regulations vary (often significantly) between jurisdictions;

[46] See *Certification Authority Liability Analysis* (study for the American Bankers Association, discussing potential liability risks of an Identity Provider operating as a certification authority); available at http://64.78.35.30/article/ca-liability-analysis.pdf.

(f) Need for legal interoperability: Identity systems are challenged by the fact that applicable laws may differ from jurisdiction to jurisdiction. In the absence of uniform laws governing their activities, identity systems often seek to address this problem by developing operating rules that provide legal interoperability to the overall system. The variation of laws and regulations among jurisdictions will challenge construction of such operating rules and other contracts that are needed to render system participant performance more uniform across online systems;

(g) Restrictions on ability to modify law by contract: Some existing laws and regulations can be modified by contract. For example, many statutes incorporate doctrines of contract or commercial law that merely establish “default rules” which apply in the absence of express choice by the parties, but permit modification of those rules by agreement of the parties to a transaction. In such cases, parties to an identity system are free to modify default rules and fill-in the blanks by the use of appropriate contract-based operating rules. In other cases, however, mandatory rules of law cannot be disregarded by mere agreement of the parties, because they serve public policy purposes such as the protection of consumers or third parties.

34. As a consequence, existing laws may create barriers to the adoption of efficient, interoperable, and trustworthy identity systems that can operate cross-border. Developing contract-based operating rules for an identity system is the primary method of addressing these legal challenges and reducing uncertainty for participants. It also facilitates experimentation with different systems and different approaches as the marketplace works to solve to the issue of identity management.

35. All participants in a federated identity system have an interest in fairly allocating, in advance, the risk of liability that flows from participation in the process, as well as mitigating those risks to the extent possible. Without addressing how that liability should be allocated, or who is in the best position to bear the risks, the existing legal uncertainties are a major barrier to the implementation of a trustworthy identity system. As identity management processes are used for more significant transactions, and the risks to the parties increase accordingly, the benefits to all parties of implementing appropriate operating rules to address those risks up front, as well as to mitigate those risks (to the extent possible) by requiring performance of specific obligations by each participant role, is significant.

36. Building private sector, cross-border, and interoperable identity systems for business transactions is the challenge that lies ahead. As with the credit card and electronic payment systems, the operating rules for identity systems are likely to be contract-based, particularly to the extent that they are intended to be deployed at internet scale across jurisdictional borders. Legislation designed to remove barriers to (rather than regulate) such systems may be appropriate for consideration.

* * *

DEFINITIONS

[*NOTE: These definitions are general in nature and are provided solely to assist in understanding the foregoing text*]

Attribute: A named quality or characteristic inherent in or ascribed to a subject, such as name, address, age, gender, title, salary, net worth, driver’s licence number, Social Security number, etc. (for a human being), make and model, serial number, location, capacity, etc. (for a device), etc. Synonyms: identity attribute

Attribute provider: An entity that acts as an authoritative source of one or more attributes of a subject's identity and is responsible for the processes associated with collecting and maintaining such attributes. An attribute provider asserts trusted, validated attribute claims in response to attribute requests from identity providers and relying parties. Examples of attribute providers include a government title registry, a national credit bureau, or a commercial marketing database.

Authentication: The process of verifying the claimed identity of a subject by confirming its association with a credential. For example, entering a password that is associated with a username is assumed to verify that the user is the person to whom the username was issued. Likewise, comparing a person presenting a passport to the picture appearing on the passport verifies or confirms that he/she is the person described in the passport.

Authenticator: Something that is used to verify the relationship between a subject and a credential; usually an object, an item of knowledge, or some characteristic of its possessor that is used to tie a person to an identity credential. For example, a password functions as an authenticator for a user ID, a picture functions as an authenticator for a passport or driver's licence.

Authorization: A process of granting rights and privileges to authenticated subjects based on criteria determined by the relying party; designed to control access to information or resources so that only those specifically permitted to use such resources are granted access to them.

Credential: Data presented as evidence of a claimed identity of a subject. Examples of paper credentials include passports, birth certificates, driver's licences, and employee identity cards. Examples of digital credentials include usernames, smart cards, and digital certificates.

Federated identity system: An identity system in which a subject can use an identity credential issued by any one of several identity providers to authenticate to multiple unrelated relying parties across different systems.

Identification: The process of collecting, verifying, and validating sufficient attribute information about a specific subject to define and confirm its identity within a specific context. (Synonyms: enrolment; identity proofing)

Identity: Information about a specific subject in the form of one or more attributes that allow the subject to be sufficiently distinguished within a particular context. The set of the attributes of a person which allows the person to be distinguished from other persons within a particular context.

Identity management: The processes, functions, and capabilities for collecting, verifying, binding, and communicating identity information about a subject to a relying party, so that the relying party can verify that such identity information corresponds to a specific subject.

Identity provider: An entity responsible for the identification of persons, legal entities, devices, and/or digital objects, the issuance of corresponding identity credentials, and the maintenance and management of such identity information for subjects. (Synonyms: credential service provider (CSP); certification authority (CA); attribute provider (where limited attribute data is provided))

Identity system: An online environment for identity management governed by a set of operating rules where individuals, organizations, services, and devices can trust each other because authoritative sources establish and authenticate their identities.

Operating rules: The business processes, technical specifications, and contractually-defined legal rules that govern the operation of a specific identity system. They are typically privately developed (e.g., by the operator of the identity system), and made binding and enforceable on the participants via contract. (Synonyms: trust framework; system rules; common operating rules; operating regulations)

Relying party: The person or legal entity that is relying on an identity credential or assertion of identity to make a decision as to what action to take in a given application context, such as to process a transaction or grant access to information or a system. (Synonym: service provider)

Subject: The person, legal entity, device, or digital object that is identified in a particular credential and that can be authenticated and vouched for by an identity provider. (Synonyms: data subject; user)