Federated Identity Management:
Balancing Privacy Rights, Liability Risks, and the Duty to Authenticate

By Thomas J. Smedinghoff[1]

[1] Thomas J. Smedinghoff is a partner in the Privacy, Data Security and Information Law Practice at the law firm of Wildman Harrold in Chicago. Mr. Smedinghoff is a member of the U.S. Delegation to the United Nations Commission on International Trade Law ("UNCITRAL"), where he participated in the negotiation of the United Nations Convention on the Use of Electronic Communications in International Contracts. He is Co-Chair of the Federated Identity Management Legal Task Force of the American Bar Association (ABA) Section of Business Law, and Chair of the International Policy Committee of the ABA Section of Science & Technology Law. He is also the author of INFORMATION SECURITY LAW: THE EMERGING STANDARD FOR CORPORATE COMPLIANCE (IT Governance Publishing, 2008). He can be reached at smedinghoff@wildman.com.

In this age of phishing, hacking, social engineering, and identity theft, the answer to the question "Who are you?" has taken on a new dimension. In an online environment, without the benefit of face-to-face personal contact, authenticating the identity of the remote party is more important than ever. It plays a key role in fighting identity fraud, is essential to establishing the trust necessary to facilitate electronic transactions of all types, and in many cases has become a legal obligation. Yet at the same time, it raises significant privacy and identity theft concerns, among others.

Verifying the identity of a person or entity[2] that seeks remote access to a corporate system, that authors an electronic communication, or that signs an electronic document, is the domain of what has also come to be called "identity management." It is increasingly playing a critical role in online commerce. As the European Commission has noted:

> Electronic Identity Management is a key element for the delivery of any e-services. On the one hand, e-identification gives individuals using electronic procedures the assurance that no unauthorised use is made of their identity and personal data. On the other hand, administrations are able to make sure that the individuals are the persons they claim to be and have the rights that they claim to have (e.g. to receive the requested service).[3]

The OECD, in its Recommendation on Electronic Authentication, has expressed a similar view, noting that:

> Electronic authentication provides a level of assurance as to whether someone or something is who or what it claims to be in a digital environment. Thus, electronic authentication plays a key role in the establishment of trust relationships for electronic commerce, electronic government and many other social interactions. It is also an essential component of any strategy to protect information systems and networks, financial data, personal information and other assets from unauthorized access or identity theft. Electronic authentication is therefore essential for establishing accountability on line.[4]

---

[2] For an example of an identity system focused on corporate identity see the Guidelines for Extended Validation SSL Certificates established by the CA/Browser Forum at http://www.cabforum.org. For a recent example of corporate identity theft, see "WVa scam is rare type of ID theft," Chicago Tribune, May 9, 2009; available at http://www.chicagotribune.com/news/chi-ap-wv-auditorscam,0,4039207.story. Identity management issues also arise in the context of verifying the identity of a device on a system or network. However, this paper will focus only on the identity of persons and entities.

[3] European Commission, "Action Plan on e-signatures and e-identification to facilitate the provision of crossborder public services in the Single Market," COM(2008) 798 final (28 November 2008); available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0798:FIN:EN:PDF

[4] Organisation for Economic Co-operation and Development (OECD) Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication, June 2007, at p. 7; available at http://www.oecd.org/dataoecd/32/45/38921342.pdf.

Identity management is also a critical building block of information security. It forms the basis for most types of access control and for establishing accountability online. Thus, it contributes to the protection of privacy by reducing the risks of unauthorized access to personal information, data breaches, and identity theft.

At the same time, however, the need to identify persons seeking online access is complicating life for individual users and consumers (who must remember or track numerous User IDs and passwords), and is becoming increasingly costly for businesses who must identify and authenticate the ever-growing number of persons and entities with whom they deal electronically. In addition, it increases privacy risks to the individuals being identified, especially as more and more entities collect and exchange an ever-increasing amount of personal data from and about such individuals, all in the name of identity management.

One approach to address the challenges of identity management that is gaining widespread attention is the concept of federated identity management. It allows businesses to, in effect, outsource the identification and authentication processes to a third party, and eases the burden on users and consumers by allowing them to use a single sign-on.

This paper will outline the basic concepts behind identity management and the developing concept of federated identity management, and then identify and examine some of the key legal risks that must be addressed to make it work. The focus will be on identity management of persons rather than devices, conducted in a business context rather than social networking setting.

To understand federated identity management, and the legal issues it raises, we begin with an overview of the basic processes involved in identity management.

1. Identity Management Basics

Although the term "identity management" is new, the concept is not. In fact, the underlying processes have been in use for many generations in an offline environment. Passports, driver's licenses, library cards, and employee ID cards are all common examples of what might be referred to as identity management systems.

While there are many definitions and numerous different approaches to identity management,[5] it essentially involves two fundamental processes: (1) the process of identifying a person ("identification"), and (2) the process of later verifying that a particular person claiming to be that previously identified person is, in fact, such person ("authentication"). Once an

[5] The OECD defines identity management (IdM) as: "the set of rules, procedures and technical components that implement an organisation's policy related to the establishment, use and exchange of digital identity information for the purpose of accessing services or resources. Effective IdM policies safeguard digital identity information throughout its life cycle – from enrolment to revocation – while maximising the potential benefits of its use, including across domains to deliver joined-up services over the Internet." OECD Working Party on Information Security and Privacy, The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers**,** DSTI/ICCP/REG(2008)10/FINAL, (June 11, 2009), at p. 4; available at http://www.oecd.org/dataoecd/55/48/43091476.pdf (hereinafter "**OECD Report**").

individual's identity is successfully authenticated, a third process, referred to as "authorization," is used by the business relying on the authentication to determine what rights and privileges are accorded to such person – e.g., whether such person should be granted access to a database, a bar, an airport boarding area, etc.

A simple and familiar example of a basic identity management process is the case of the employee who logs into his or her employer's network using a user ID and password. Before a company allows a person to access its internal network, that person must be properly identified in a manner appropriate for the transaction (e.g., as an employee with certain authority), and then that identity must be authenticated at the time of each transaction. Employees are identified by their employer, and an identity credential containing [or consisting of] a unique identifier (typically a User ID) and other relevant information attributes is created and stored on the company's computer system. A secret (in this case, a password), is then used to link the employee to the identity credential. Thereafter, when the employee wants to remotely access the company's network, he or she can be authenticated by using the password in an authentication protocol. The authentication protocol allows the employee to demonstrate to the employer that he or she has or knows the secret, and thus, is the person previously identified.

Before proceeding, however, let us look more closely at the nature of the identification and authentication processes that form the foundation of identity management, as a clear understanding of those processes is important to the legal analysis.

(a) Identification

The ***identification*** process is designed to answer the question "who are you?" It involves associating one or more ***attributes***[6] (*e.g.*, name, height, birth date, SSN, employer, home address, passport number) with a person in order to identify and define that individual to the level sufficient for the contemplated purpose. Sometimes called "identity proofing," "identity vetting," or "enrolment," this process is usually a one-time event. It typically involves the collection of personal information about the person to be identified, and often relies on a patchwork of documents from birth certificates and Social Security cards to driver's licenses and passports.[7] The personal information may be collected directly from the person being identified, as well as from third party sources (e.g., government agencies, credit agencies, public record databases, etc.). Note that the attributes may be permanent (e.g., date of birth) or temporary (e.g., current employer), inherited (e.g., DNA), acquired (e.g., educational degrees), or assigned (e.g., employee number).

"Selected attributes are used to establish an identity – off line or on line – and can be said to uniquely characterise an individual within a system or organisation although they may differ

[6] Personal information concerning a specific category or characteristic of a given identity, such as name, address, age, gender, title, salary, health, net worth, driver's license number, Social Security number, etc.

[7] Industry Advisory Council Transition Study Group, "Identity and Access Management," (December 9, 2008) at p. 4; available at www.actgov.org/knowledgebank/studies/Documents/Transition%20Study%20Group%20Papers/Identity%20and%20Access%20Management,%20IAC,%2012-9-2008.pdf (hereinafter "**Transition Study Group Report**").

in character and number depending on the context. This context-specific notion of identity is sometimes referred to as "partial" identity."[8]

"The verification requirements for enrolment can be fulfilled entirely on line or include an offline component, for example, mailing a verification code to the individual's residence. More stringent enrolment processes may require the presentation in person of physical credentials issued to the person by other entities. These may include government-issued credentials (e.g., passports, identity cards and drivers licenses) and/or credentials issued by private sector entities (e.g., employee badges, mobile wireless SIM cards, and credit cards). Government institutions such as motor vehicle departments and post offices sometimes accomplish identity verification through this type of "in-person" proofing." In addition, in-person proofing is common among banks, schools, and employers in their enrolment processes."[9]

The process of identifying a person can vary widely across two different dimensions. The first dimension relates to the scope of the personal information attributes collected about and associated with an individual to establish his or her "identity" – i.e., which and how much information is collected and verified. A second dimension of the identification process relates to the degree of certainty with which the identifying attributes are ascertained – i.e., how accurate is the information likely to be.

(1) Scope of Information Collected

The amount and type of personal information that is required will, of course, depend on the purpose of the identification. In some cases, only minimal information is required, and the process can be limited to verifying only a very few attributes, such as "this person is over 21 years old" or "this person is a member of the group entitled to admission." This might be the case, for example, for some activities (such as purchasing wine) where a single attribute (e.g., age) might be sufficient. Generally, the fewer the attributes collected, the lower the privacy risk.

At the other end of the spectrum, it may be necessary to collect a large number of very detailed identifying attributes, such as name and address, physical characteristics, gender, race, Social Security number, employment details, criminal background, credit and financial history, medical history, and information about prior activities and transactions. This might be necessary in certain cases to ensure uniqueness, or in cases where a person is being considered for employment in a very sensitive position or for access to a very sensitive database, and a much more detailed form of identification is required to determine whether authorization should be granted. Of course, this also tends to increase the privacy risk to all parties.

(2) Accuracy of Information Collected

The second dimension of the identification process focuses on the accuracy of the identifying attributes. This is largely a function of the reliability of the source of the data and the trustworthiness of the person or system verifying the information. For example, identifying

[8] OECD Report at p. 6.

[9] OECD Report at p. 7.

attributes (such as name, address, date of birth, or SSN) might be "verified" simply by asking the person being identified to provide the information. Alternatively, they might be verified by reference to an authoritative third party source of information, such as a driver's license, passport, or other government issued identity card, or even double-verified by checking with third-party sources. Obtaining the information from an individual "in person" is also generally considered more reliable than cases where it is done remotely. But in all cases the issue is, in essence, a question of trust – i.e., how much do I trust the veracity of the information provided? It is measured by reference to an assurance level, discussed below.

One commentator has described four key verification facts that must be considered to determine the reliability of this identity vetting process:[10]

- What identity information is being verified (e.g., driver's license, passport, library card or group membership card)?
- Who is performing the verification (person or system) and to what extent can they be trusted?
- How is the verification performed – i.e., what is the process used to verify the authenticity of the identification documents?
- What is the source of the identification information and the level of diligence in creating it?

(3) Issuance of Credential

At the end of the identification process, a person's identity is typically represented by data in a paper or electronic document referred to as an identity ***credential***. A credential is data that is used to authenticate the claimed digital identity or attributes of a person.[11] In the physical world, the identity credential may be a driver's license, a passport, a library card, or an employee identification card. In the online world the identity credential may be as simple as a User ID, or as complex as a cryptographically-based digital certificate. [Examples of digital credentials include: an electronic signature, a password, a verified bank card number, a digital certificate, or a biometric template.]

Electronic identity credentials typically contain a unique ***identifier*** (such as name, user ID, account number, Social Security number, etc.) along with the relevant attributes that describe or define the person to the level necessary for the purpose at hand (e.g., address, title, gender, status, date of birth, credit score, medical information, etc.). In addition, identity credentials are often associated with an ***authenticator*** (also called a ***token***) possessed and controlled by the person identified in the credential. The token assures that the credential can be reliably associated with the specific person about whom it relates. The token can be digital information, such as a secret known only to the individual (e.g., a password), or a physical object such as a

---

[10] Jacques R. Francoeur and Edward Chase, "Digital Signature Assurance & the Digital Chain of Evidence," Version 1.0, January 2009, at p. 14; [copy on file with author]

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

smartcard or ATM card. The token and credential may then be used in subsequent authentication events.

With respect to both of the dimensions of identification, the nature of the process is critical. Before someone relies on an identity that is based on the results of an identification process, they need to be able to trust that the process is both appropriate for the task and that it was accurately conducted. Likewise, following completion of the identification process, the continuing security of the data and the authenticating token is also a critical concern. If a new photo can be pasted into a driver's license, or if a password is lost or stolen, an identity thief can successfully claim to be the person identified by the credential created during the identification process.

(b) Authentication

"When an individual seeks access to an organisation's systems, he or she "***authenticates***" him or herself by providing the credential issued during the enrolment process. The authentication process provides a level of assurance as to whether the other party is who they claim to be. The level of assurance and associated authentication credentials required depends on the level of risk inherent in the transaction or interaction."[12]

When a person presents an identity credential (such as by using a User ID on a corporate network, or presenting a driver's license at an airport), claims to be the individual identified in the credential, and seeks to exercise a right or privilege granted to the individual named in the credential (e.g., to access the network or a sensitive database, to board a plane, etc.), an ***authentication*** process is used to determine whether that person is, in fact, who they claim to be.[13] In other words, once someone makes a declaration of who they are, authentication is designed to answer the question "OK, how can you prove it?" In essence, it is the process of establishing confidence in a person's claimed identity.

Typical legal definitions of authentication include: "the corroboration that a person is the one claimed,"[14] "utilizing digital credentials to assure the identity of users and validate their access,"[15] and a "procedure for checking a user's identity."[16] It is a transaction-specific event that involves verifying that the person trying to engage in the transaction really is the person that was previously identified and authorized for the transaction.

There are a variety of technologies and methodologies to authenticate individuals. These methods include the use of passwords, personal identification numbers (PINs), digital certificates

---

[12] OECD Report at p. 7.

[13] *See* U.S. Federal Rules of Evidence 901(a). *See also*, Federal Trade Commission Report, "Security in Numbers: SSNs and ID Theft" (FTC, December 2008), at p. 6; available at http://www.ftc.gov/opa/2008/12/ssnreport.shtm.

[14] HIPAA Security Regulations, 45 C.F.R. Section 164.304.

[15] Homeland Security Act of 2002 § 1001(b), amending 44 U.S.C. § 3532(b)(1)(D).

[16] Spain, Royal Decree 1720/2007 of 21 December, Which Approves The Regulation Implementing Organic Law 15/1999, of 13 December, on the Protection of Personal Data, Article 5(2)(b).

using a public key infrastructure (PKI), physical devices such as smart cards, one-time passwords, USB plug-ins or other types of "tokens," transaction profile scripts, biometric identification, and others.[17]

In all cases, however, authentication is essentially performed by cross-checking a claimed identity against one or more authenticators, often referred to as "tokens," that are associated with or linked to that identity. An authenticator (or token) typically consists of one of the following *factors*:

- Something the person *knows* (e.g., a secret such as a PIN, password or other secret code);[18]
- Something the person *possesses* (e.g., a cryptographic key, an ATM card, a smart card, drivers license, or other physical token); or
- Something the person *is* (e.g., a biometric characteristic,[19] such as a fingerprint or retinal pattern).

For example, when someone presents a driver's license, the biometric characteristic that comprises his face (something he "is") can be compared to the picture embedded in the license, and if they match, the person's claimed identity (e.g., name, age, etc. as stated on the license) is authenticated. Likewise, in the online environment, when an employee logs into the company network, his password (something he "knows") is checked against the password associated with his identity credentials stored on the company's server, and if they match, the employee's claimed identity (represented by the identifier known as a user ID) is authenticated.

Authentication processes may require one or more of these factors. The online use of a password is *single factor authentication* (i.e., something the user knows), whereas an ATM transaction requires *two factor authentication* – i.e., something the user possesses (the ATM card) combined with something the user knows (the PIN number).[20] Properly designed and implemented multi-factor authentication methods typically are more difficult to compromise than single factor systems. As a result, they are more reliable indicators of authentication and stronger fraud deterrents.

---

[17] Federal Financial Institutions Examination Council ("FFIEC"), "Authentication in an Internet Banking Environment," October 12, 2005, at p. 2; available at http://www.ffiec.gov/pdf/authentication_guidance.pdf (hereinafter "**FFIEC Guidance**").

[18] The use of a user name or user ID, coupled with a secret string of characters such as a password or PIN, is one of the most common authentication methods. The security provided by user IDs and passwords is, of course, dependent upon the password being kept a secret.

[19] A biometric identifier measures an individual's unique physical characteristic or behavior and compares it to a stored digital template to authenticate the individual. Thus, it represents "something the user is." Commonly used biometrics include a person's voice, fingerprint, hand or face geometry, the iris or retina in an eye, or the way the person signs a document or enters key board strokes. The security of a biometric identifier rests on the ability of the digitally stored characteristic to relate to only one individual in a defined population.

[20] FFIEC Guidance, at p. 3.

Once a user has successfully authenticated him or herself to a system, an ***authorization*** process controls what the user is allowed to access and use. It addresses the question "What can I do?" In other words, authentication of identity is not just an end in itself, but rather a process used to authorize some type of grant of rights or privileges (e.g., to access and use certain system resources), to facilitate a transaction or decision, or to satisfy an evidentiary obligation. For example:

- With respect to *computer systems and networks*, authentication is often used for access control – e.g., to determine who is seeking access in order to ensure that only authorized persons are given the right to access a database of sensitive personal information or the right to transfer funds out of a bank account. As such, it can play a critical role in protecting the privacy and confidentiality of data stored on corporate networks.[21]

- With respect to *electronic communications*, authentication of identity can be used to assure the recipient of a message that the sender is who he or she (or it) claims to be so that the recipient can determine whether to proceed with the transaction. For example, when a bank receives an electronic payment order from a customer directing that money be paid to a third party, the bank must be able to verify the source of the request and ensure that it is not dealing with an impostor. This is a critical defense against identity theft.

- With respect to signed *electronically signed records*, authentication might be used to verify the identity of the signer. Someone seeking to enforce an electronic promissory note, for example, must be able to authenticate the identity of the signer. In this case, it serves an important evidentiary function.

In all cases, note that there is a clear difference between identification and authentication. *Identification* is the process of verifying a person's identity to a level sufficient for the intended purpose (such as during the hiring process or an account origination process) and usually occurs once. *Authentication* is the process of confirming that a person presenting him or herself as a previously identified person entitled to certain rights and privileges is, in fact, that person (such as when a person attempts to gain access to an online system), and typically occurs at the time of each transaction.

(c) Assurance Levels and Privacy

Both identification and authentication are critical to access control and to otherwise stopping identity theft. Without reliable identification, one person can pose as another, and obtain an identity credential in another's name. And even with proper identification, if the authentication process fails – e.g., when an imposter successfully presents himself as someone else by using a stolen password – identity theft can occur. In other words, there are two basic

[21] That is, it helps to keep out unauthorized persons. It does not, however, prevent authorized persons from misusing their access rights, although it does help provide an audit trail that can detect misuse of such data by identifying who accessed the compromised data.

ways an identity thief can succeed: (1) by foiling the identification process, or (2) by foiling the authentication process.

With respect to the identification process, there is always the risk someone can misrepresent his or her identity, and if successful, obtain an identity credential in the name of someone else. For example, John Smith might claim that he is Bill Gates of Microsoft (e.g., by presenting false identification documents), and fraudulently obtain an identity credential asserting that he is, in fact, Bill Gates, along with a corresponding password or other token to authenticate such identity. Thus, the reliability and proper performance of the identification process is critical to the identity management process.

With respect to the authentication process, there is the risk that, although a person was correctly identified based on legitimate documentation, the password or other token used to link that person to the resulting accurate identity credential might be compromised, thereby allowing an imposter to successfully complete the authentication process and steal such person's identity. For example, if the real Bill Gates of Microsoft was properly identified and issued an identity credential, and that identity credential was associated with a token that was compromised (e.g., a stolen password), then the possessor of the stolen password would be able to pose as Bill Gates. Thus, the reliability and proper performance of the authentication process is critical to the identity management process.

In light of these risks, a person relying on an authenticated identity (e.g., a bank relying on an authentication of Bill Gates to permit a transfer of funds out of the Microsoft account) must also consider the degree of confidence or trust that it has in both the identification and authentication processes. This is sometimes referred to as the "assurance level."

The "assurance level" describes the ***strength*** of the identification and authentication processes – i.e., it provides a basis for determining the degree to which a party to an electronic business transaction can be confident: (1) that the identity information being presented actually represents the person named in it (e.g., that the person who was identified as Bill Gates really was Bill Gates, and not an imposter), and (2) that the person identified in the credential is the person who is actually engaging in the electronic transaction (e.g., that it is really Bill Gates on the remote device who is seeking access to a company's system, and not someone who stole his password).[22]

The U.S. Federal government has defined four levels of assurance to describe the degree of certainty associated with identification and authentication processes. The four assurance levels range from little or no confidence in the asserted identity's validity (level 1), to some confidence (level 2), to high confidence (level 3), to very high confidence in the asserted

[22] See, e.g., Liberty Alliance Project, Liberty Identity Assurance Framework, Version 1.1 (2008), at page 7; available at http://www.projectliberty.org/resource_center/specifications/liberty_alliance_identity_assurance_framework_iaf_1_1_specification_and_associated_read_me_first_1_0_white_paper (hereinafter "**Liberty Identity Assurance Framework**"); Office of Management and Budget, **"**E-Authentication Guidance for Federal Agencies," OMB Memo M-04-04, (December 16, 2003), at Section 2.1; available at http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf (hereinafter "**OMB Memo M-04-04**).

identity's validity (level 4).[23] Since the assurance level is a function of the strength of the processes and the technology used in connection with the identification and authentication, the primary factors that affect the assertion level include:[24]

- The nature of the identity proofing processes: What was done do to vet the person's identity? – e.g., What kind of identity credentials were relied upon (e.g., passport or library card)? Was the process done in-person or remotely via the Internet?
- The tokens used: What kind of tokens were used for proving identity and how strong or reliable are they? – e.g., weak passwords, strong passwords, one-time password device tokens, cryptographic keys stored in hardware devices, etc.?
- The remote authentication mechanisms used: What is the combination of credentials, tokens and authentication protocols[25] used to establish that a claimant is in fact the person he or she claims to be? – e.g., how resistant are they to eavesdroppers, imposters, and hijackers?

Obviously, different types of transactions will require different assertion levels, and not all transactions will require the highest assertion level. However, the confidence level that a business has in a particular identity, and its willingness to proceed with the transaction (e.g., to transfer the funds) or grant the requested privilege (e.g., access to a sensitive database) is clearly tied to assurance levels in some form. And the greater the risk of the transaction the greater the assurance level must be. Thus, in many developing identity management systems there is a focus on the strength of the identification and the authentication processes, even if not evaluated formally in terms of assurance levels.[26]

A practical problem, however, is that achieving a higher assurance level often requires obtaining more personal information, thereby increasing the privacy risk. For while the strength of the identity credential and the authentication mechanism can be addressed technically (e.g., a hardware-based digital certificate is stronger than a mere password), the strength of the identification (or the identity proofing) is often a function of the amount of personal data collected about an individual. As one commentator has noted:

> Reliability of identity can be built up from a series of credentials and records . . . . This is an example of the principle that many bits of somewhat reliable data may aggregate into a bit of quite reliable information. If an individual presents a driver's license, automobile registration and insurance card for the same vehicle,

---

[23] OMB Memo M-04-04, Section 2.1.

[24] See, e.g., National Institute of Standards and Technology, "Electronic Authentication Guideline," Special Publication No. 800-63, Version 1.0.2, (April, 2006) at p. 2; available at http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf (hereinafter "**NIST Special Publication 800-63**").

[25] "An authentication protocol is a defined sequence of messages between a claimant and a verifier that enables the verifier to verify that the claimant has control of a valid token to establish his/her identity. An exchange of messages between a claimant and a verifier that results in the authentication (or authentication failure) of the claimant is a protocol run." NIST Special Publication 800-63, at p. 26.

[26] See, e.g., NIST Special Publication 800-63; Liberty Identity Assurance Framework.

> all of which have the same name and address, that is, if they are mutually referential, a much stronger case can be made that the series of credentials reliably defines an identity. Add a mortgage account, a checking account, voter registration records, medical insurance account, and the overall confidence one has in the individual's identity grows even greater. Add to this list access to medical records (undesirable for reasons other than identity proofing, but then we are speaking here in the abstract) and credit history and the confidence in the individual's identity rapidly rises towards certainty, that is, the electronic credential issuer is just about 100% sure the individual presenting all these credentials – onerous as that surely would be – is who he or she claims to be.[27]

It should be noted, however, that the strength of the identity is also dependent on proper performance of the identity proofing and authentication processes. Because the assurance level determination focuses on the nature of the process and technology, and not on the risk that a participant will fail to perform its obligations, it does not necessarily address the performance risk discussed below (e.g., although an identification process may require an in-person review of two government-issued picture IDs, a willingness to circumvent that process and issue an identity credential based only on a telephone claim of identity will defeat the strength of that identity-proofing process).

2. The Next Generation – Federated Identity Management

Traditionally, each business entity and government agency has handled its own identity management. For example, a company would identify each of its employees and customers, and then assign each of them a unique identifier (typically a user ID) tied to an internal identity credential, and associate an authenticator or token (typically a password) to that User ID and identity credential, so that those persons could be authenticated for remote network access. Only two parties are involved in this type of identity management process – the business and the individual to be granted access.

Today, however, businesses and government agencies increasingly want to: (1) use third parties to handle the difficult and often expensive tasks involved in identity management, particularly in situations involving high volume or one-off transactions, or (2) leverage the identification and authentication previously done by a related business (e.g., a hotel and car rental company might want to rely on an airline's identification of a traveler). In addition, users, overloaded with user IDs and passwords are looking for a one-stop option. This is where a three-party identity management model, known as *federated identity management*, offers a promising solution for dealing with the cost and complexity of addressing these identity management problems.

Under a federated identity model, a business relies on an identification process performed, and identity information provided, by a third party. The goal is to facilitate the secure exchange of identity credentials between organizations – i.e., to enable the portability of

[27] Peter Alterman, "On the Reliability of Authentication of Identity," at pp. 4-5, 7; available at http://www.cio.gov/fpkipa/documents/ReliabilityAuthenticationIdentity.pdf

identity information across different systems and entities. Thus it "allows individuals to use the same user name, password, or other personal identification to sign on to the networks of more than one enterprise in order to conduct transactions."[28]

Federated identity management (FIM) has been generally summarized by Ann Cavoukian, the Information and Privacy Commissioner of Ontario, as follows:

> Within the FIM model, identity credentials issued to a user by a particular service or institution are recognized by a broad range of other services. Though complex to implement online, this is similar in concept to, and can provide improvements over, traditional identification schemes in the "physical world." A typical example would be government-issued ID credentials (birth certificate, driver's license, passport, citizenship card, etc.), issued by an institution (a government agency), that is broadly recognized by others (as proof of name, address, age, etc.). The user of the service does not need to prove his/her identity with each transaction; rather, it is enough to show that he/she has, at some prior point, been authenticated by a trusted authority. The service's burden then lays, not in identification of the presenter but in the verification of presented credentials – a much less onerous task.[29]

Much work is being done by groups such as the Liberty Alliance,[30] the Organization for the Advancement of Structured Information Standards (OASIS),[31] the World Wide Web Consortium (W3C),[32] and others to develop technical specifications and online protocols that allow a business to authenticate the identity of a person seeking to access its systems by obtaining and validating online identity information provided by a third party. Most of that work, however, focuses on the practical and technical issues of communicating identity-related information in an inter-operable manner. The legal issues associated with federated identity management are often overlooked and have not been the subject of much discussion to date.

(a) The General Process

While there are many different approaches to federated identity management, and the technical details and specifications of each approach can become quite complex, the following oversimplified summary of the process will help to put the legal issues in perspective:

- A business or a government agency (the ***Relying Party***) wants to (1) authenticate the identity of a particular person (the ***Subject***), and (2) obtain certain information about the Subject (an ***identity assertion***) before it allows the Subject to access its system or enter

[28] Liberty Identity Assurance Framework, at p. 119.

[29] Information and Privacy Commissioner of Ontario, "The New Federated Privacy Impact Assessment (F-PIA): Building Privacy and Trust-enabled Federation" (January, 2009), at p. 4; available at http://www.ipc.on.ca/images/Resources/F-PIA_2.pdf (hereinafter "**Privacy Commissioner of Ontario Paper**").

[30] http://www.projectliberty.org

[31] http://www.oasis-open.org

[32] http://www.w3.org

into a proposed business transaction. The Subject may, for example, be a customer seeking access to the Relying Party's network, a person seeking to enter into an online contract with the Relying Party, or someone seeking to access their financial account with the Relying Party. The information the Relying Party needs may be the Subject's account number, Social Security number, address, or membership status.

- To provide the required identity information, and facilitate the authentication process, a third party (called the ***Identity Provider***) must have previously identified the Subject and issued a digital identity credential to facilitate authentication of the Subject. The Identity Provider will then be asked to make an identity assertion about the Subject that contains the requested information.

- At the time of the transaction, the Subject is first authenticated by the Identity Provider[33] and then the identity assertion is communicated to the Relying Party (by either the Subject or the Identity Provider, depending on the system involved), the Relying Party validates the identity assertion to ensure that it is authentic and not revoked, and then relies on it to obtain the necessary information in order to grant access to a network or proceed with the proposed transaction.

A very common offline example of this federated identity process (although it was never intended as such) is the way we currently issue and use driver's licenses. Obtaining a driver's license begins with an in-person identification process conducted by a state's Department of Motor Vehicles (the Identity Provider), whereby selected identifying information (or attributes) about a person, such as name, address, date of birth, height, weight, and eye color, are collected and verified. Then following testing of eyesight and driving competence, the process culminates with the issuance of a driver's license (an identity credential) that identifies the individual with a unique driver's license number (the identifier), contains some of the identity attributes about the individual that were collected during the identification process (identity assertions), and includes a photograph of the person named in the license that was taken at the time the license was issued. The photograph functions as an authenticator – i.e., it is used to tie the person to the identity credential.

The person obtaining that license may later present it to a Relying Party (such as a TSA agent at an airport, or the bartender at a bar), claiming to be the person with the identity attributes stated on the driver's license. That third party will then attempt to verify that the person standing in front of him is the same person identified in the license by comparing the photo on the license to the person before him – i.e., he will attempt to "authenticate" the claimed identity asserted by that person. If successful, he will typically be willing to rely on the data stated in the identity credential (the identity assertions) for purposes of a transaction with such person. The bartender,

---

[33] Authentication can occur in various ways: the Relying Party can initiate an authentication request to the Identity Provider the Subject designates when logged onto an Relying Party, or the Subject can first authenticate at an Identity Provider and then access a Relying Party. In either case, the technology enables single sign-on in which the Identity Provider authenticates the Subject, thus allowing her access to protected resources at a Relying Party. Susan Landau, Hubert Le Van Gong, and Robin Wilton, "Achieving Privacy in a Federated Identity Management System,**"** (2009) at Section 1.1; available at http://research.sun.com/people/slandau/Achieving_Privacy.pdf (hereinafter "**Landau Article**").

for example, will rely on the identity assertion regarding age stated in the license to determine whether to serve alcohol to the license holder; the TSA agent will rely on the identity assertion regarding name stated in the license for purposes of determining whether such person is the same as the person named in the airline boarding pass, and thus entitled to enter the boarding area.

(b) Online Examples

In the traditional two-party identity management system, the Identity Provider and the Relying Party are the same entity. For example, a business will identify its employees, and issue them user IDs and passwords so that the employees can access the company's network. In that case, the company fills the role of the Identity Provider as well as the role of the Relying Party.

On the other hand, when that same business provides a link (via the company intranet) to a third party managing the retirement accounts for its employees, and its employees are able to access their retirement accounts without entering an additional user ID and password, a federated approach to identity management is in place. In that scenario, the company acts as the Identity Provider (i.e., it identifies its employees and authenticates them when they sign on to the company network at work), and the third party manager of the retirement accounts is the Relying Party. It relies on the identity assertions made by the company to allow the company's employees (who have signed on to the company network) to have seamless access to their benefit accounts.

Another example of a federated identity arrangement (in a closed system) is the typical ATM transaction whereby an individual with an account at Bank A wants to obtain cash from an ATM machine operated by Bank B (with whom he has no relationship). The individual signs on to Bank B's ATM network using his ATM card and password from Bank A. Through the ATM network, Bank B contacts Bank A 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 he enter the correct password), and to obtain certain identity information about the individual from Bank A (e.g., whether his account has funds sufficient to cover the requested withdrawal, and the balance in his account so Bank B can print it on the transaction receipt).

In the future, a federated identity arrangement might allow a government agency, such as the Social Security Administration (as a Relying Party), to authenticate the identity of an individual (the Subject) seeking access to his or her SSN records by relying on an identity assertion made by that person's bank (which has previously identified that Subject as part of its customer screening process, and thus is in a position to function as an Identity Provider). For the individual Subject, the online process would be simple. He might simply sign onto the SSA website using the user ID and password he uses to access his online bank account. The SSA would then send a message to the bank to verify that the individual's User ID and password is still valid, and to obtain an identity assertion from the bank that contains certain information confirming the Subject's identity (such as his SSN). Then, when the process is completed and his identity authenticated, the SSA will grant him access to check his records or to redirect the automatic deposit of his Social Security payments. So long as a protocol exists for sharing the identity data between the bank and SSA, an individual can do business with SSA using the user ID and password (or other identity credential) issued by his bank, and the SSA can avoid the need for a costly identity proofing process for all citizens.

That assumes, of course, that SSA trusts the identification process used by the bank, that the bank can limit to a reasonable level its liability risk should it make a mistake, and that the individual involved (the Subject) trusts both the bank and the SSA to properly use and protect the personal information he or she initially provided to the bank. These issues, among others, are some of the key legal problems that the parties involved in the process of federated identity management must address.

3. The Key Legal Risks

The challenges of the federated identity management fall into three general categories. First are the technological and procedural challenges, such as implementing the required technology and establishing appropriate processes and procedures so that everything works properly, ensuring the inter-operability of identity assertion communications between Identity Providers and Relying Parties, and ensuring the security of Subject identity information. The second challenge is economic, and involves primarily dealing with the cost of deploying, coordinating, and using identity management systems. The third challenge is legal. As suggested by the SSA example above, it focuses on issues relating to the privacy and security of the Subject's identity information, the potential liability of the Identity Provider in issuing identity credentials and making identity assertions, the needs of the Relying Party for legally sufficient authentication, and the mutual concerns of all participants (Subject, Identity Provider, and Relying Party) that everyone perform their obligations properly. This third category is the focus of the following discussion.

The legal risks in a federated identity management system are all centered around issues raised by the collection, verification, use, communication, and security of personal information. But they are not all strictly "privacy" issues. Rather, they tend to fall into the following four categories:

- Privacy risk
- Authentication risk
- Liability risk
- Performance risk

Each of these risks affect all of the roles in a federated system (Subjects, Identity Providers, and Relying Parties), although perhaps in different ways. Thus, each role may well have potentially conflicting needs and goals with respect to addressing these risks.

(a) Privacy Risk

By its nature, any form of federated identity management involves the collection (by an Identity Provider) and disclosure (to a Relying Party) of personal information about a Subject. Thus, "the foundational issue in approaching any [identity management] system is personal information – how it is collected, stored, shared, and used."[34] Moreover, by its nature, federated

[34] Office of Science and Technology Policy (OSTP), National Science and Technology Council (NSTC), Subcommittee on Biometrics and Identity Management, "Identity Management Task Force Report 2008,"

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.[35]

For Subjects, protecting the privacy and security of their personal information is a primary concern. At the same time, however, the other roles have needs that potentially conflict with the Subject's privacy rights. For Identity Providers, the right to collect, process, and exchange this personal information is critical to the identity services they provide, and thus, they have a major interest in ensuring their continued ability to do so. Likewise, Relying Parties often need the ability to receive, process, and use at least some of this information for the transaction they are entering into with the Subject.

The privacy risk for Subjects focuses on the protection and use of their personal information by Identity Providers, Relying Parties, and other third parties, the resulting possibility of inappropriate use, disclosure, and compromise, and the harms that may result, such as identity theft, unauthorized account access, embarrassment, etc. And this risk relates not only to the information provided by the Subjects, but also information about the Subjects collected from third parties, as well as metadata and transaction data about Subjects generated as a result of their online activities.

To benefit from participation in a federated identity system, Subjects must disclose personal information, and thus expose it to risk. Yet a vital part of maintaining their confidence in the process is ensuring that the personal information that Identity Providers collect about Subjects during the identification process, and disclose to Relying Parties during the authentication processes, is verified, maintained in an accurate and up-to-date form, kept private, not shared with third parties, and not misused or exposed to unauthorized individuals, such as identity thieves. Thus, questions of potential significance to Subjects generally include:

- Who is collecting information about them?
- What information is being collected?
- Where is the information being collected from?
- Why is the information being collected?
- How is the accuracy of the information verified?
- What steps are taken to ensure that the information remains accurate and up-to-date?
- Where is the information being processed and stored?
- With whom the information will be shared?
- What use will be made of the information (by the Identity Provider, any Relying Parties with whom the information is shared, and any other parties that may ultimately have access to it)?

(September 2008) at p. 16; available at http://www.ostp.gov/galleries/NSTC%20Reports/IdMReport%20Final.pdf (hereinafter "**OSTP Report**").

[35] Privacy Commissioner of Ontario Paper, at p. 7, 13.

- What opportunities do Subjects have to decline to provide information, or to consent to or prohibit particular uses of the information?
- How the information is secured?
- How long is the information retained, and how is it destroyed?
- What are their rights in the event that their information is misused?

For Identity Providers and Relying Parties, the privacy risk involves navigating the challenges of compliance obligations and restrictions that might inhibit their ability to achieve their goals. Laws and regulations may regulate or restrict their collection and use of personal information, as well as impose a variety of obligations to protect the information.[36] In addition, restrictions on cross-border transfers and other forms of use or sharing of such information may have an impact. Failure to address these obligations may result in penalties and fines, as well as potential liability for any harms suffered by the Subjects themselves.

Identity Providers and Relying Parties are also concerned about obtaining (or retaining) the rights necessary to do what is required to satisfy their obligations in the identification and authentication processes (as well as their right to use the personal information for other related, or unrelated, business purposes). At the same time, they are also concerned about limiting their liability exposure in the event of a misuse or breach of the personal information in their possession. This is often a difficult balancing act in an identity management context, as collecting and holding too much personal data may expose them to disproportionate liability or an excessive burden of compliance; while at the same time, collecting too little personal data can itself lead to liability exposure in certain contexts, such as money laundering or providing healthcare services.

Part of the solution for all parties may well lie in establishing a set of rules that govern the privacy and security of that personal information (and allocating the related liability risks) in a manner acceptable for all participants.

(b) Authentication Risk

If personal information is the foundation of any identity management system, the exchange of that information between organizations, for the purposes of remote authentication of identity and the related communication of identity assertions, is clearly the goal of identity management. Without the ability to remotely and reliably authenticate identity and provide appropriate identity assertions, the trust necessary for online transactions is missing. Thus, the success of the authentication process and the reliability of the identity assertion is a key concern both for Relying Parties (who need to know who they are dealing with) and for Subjects (who want to be sure that they are able to complete an online transaction, and that identity thieves are not).

For Subjects the authentication risk is both a business concern (will I be able to complete this online transaction, access this database, etc.?), and privacy concern (will someone be able to

[36] This includes, e.g., GLB, HIPAA, state data security laws, etc., as well as the data protection laws in other countries, including the EU, Argentina, Australia, Canada, Hong Kong, Japan, and South Korea.

use my identity to successfully complete this transaction in my name?). For Identity Providers, the authentication risk relates to the possibility that its faulty identification or authentication processes will result in an improper identification and subsequent harm to the Relying Party and/or the Subject, with the consequence that the Identity Provider will be liable for the damages incurred.

For Relying Parties, authentication risk is both a liability concern (focused on the losses it will suffer if it relies on an inappropriate authentication or identity assertion), as well as a legal compliance obligation. From a liability perspective, the Relying Party needs the assurance or trust necessary to enter into a particular online transaction, as well as some level of confidence that it can prove up the identity of the other party in court if that becomes necessary. At the same time, however, laws and regulations increasingly impose on businesses a duty to identify and authenticate the persons with whom they deal remotely. Thus, for many Relying Parties identity management has become a legal obligation.

In many cases, the obligation is imposed by law or regulation. One prominent example is the requirements for authentication in online banking activities set forth in a guidance document issued by the FFIEC[37] in late 2005 titled "Authentication in an Internet Banking Environment" ("FFIEC Guidance").[38] The FFIEC Guidance makes clear that "Financial institutions offering Internet-based products and services to their customers should use effective methods to authenticate the identity of customers using those products and services."[39] Expanding on the rationale for this requirement, the FFIEC points out that:

> An effective authentication system is necessary for compliance with requirements to safeguard customer information,[40] to prevent money laundering and terrorist financing,[41] to reduce fraud, to inhibit identity theft, and to promote the legal

---

[37] Federal Financial Institutions Examinations Counsel. The FFIEC is a formal U.S. interagency government regulatory body empowered to prescribe uniform principles, standards, and report forms for the federal examination of U.S. financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS), and to make recommendations to promote uniformity in the supervision of financial institutions. See http://www.ffiec.gov

[38] Federal Financial Institutions Examination Council ("FFIEC"), "Authentication in an Internet Banking Environment," October 12, 2005, at p. 2; available at http://www.ffiec.gov/pdf/authentication_guidance.pdf (hereinafter "**FFIEC Guidance**").

[39] FFIEC Guidance, at p. 1. Other countries, such as Singapore, have also adopted similar requirements. Monetary Authority of Singapore, Circular No. SRD TR 02/2005, 25 November 2005.

[40] "The Interagency Guidelines Establishing Information Security Standards that implement section 501(b) of the Gramm–Leach–Bliley Act, 15 USC 6801, require banks and savings associations to safeguard the information of persons who obtain or have obtained a financial product or service to be used primarily for personal, family or household purposes, with whom the institution has a continuing relationship. Credit unions are Subject to a similar rule." FFIEC Guidance, at fn. 3.

[41] "The regulations implementing section 326 of the USA PATRIOT Act, 31 USC § 5318(l), require banks, savings associations and credit unions to verify the identity of customers opening new accounts. See 31 CFR 103.121; 12 CFR 21.21 (OCC); 12 CFR 563.177 (OTS); 12 CFR 326.8 (FDIC); 12 CFR 208.63 (state member banks), 12 CFR 211.5(m) (Edge or agreement corporation or any branch or subsidiary thereof), 12 CFR 211.24(j) (uninsured branch, an agency, or a representative office of a foreign financial institution operating in the United States (FRB); and 12 CFR Part 748.2 (NCUA)." FFIEC Guidance, at fn. 4.

> enforceability of their electronic agreements and transactions. The risks of doing business with unauthorized or incorrectly identified persons in an Internet banking environment can result in financial loss and reputation damage through fraud, disclosure of customer information, corruption of data, or unenforceable agreements.[42]

The FFIEC's reference to "requirements to safeguard customer information" identifies another key source of authentication requirements. That is, the many laws and regulations that impose on a company a duty to provide reasonable security for its data[43] typically include (expressly or impliedly) an obligation to properly authenticate persons seeking to access its data, networks or services. In addition to the GLB security regulations referenced by the FFIEC,[44] other examples of the express duty to authenticate include:

- the HIPAA security regulations, which require covered entities to "implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed;" [45]
- state information security laws, such as Massachusetts, which requires the use of "secure user authentication protocols" and "secure access control measures," and California, which requires "reasonable security procedures and practices . . . to protect the personal information from unauthorized access . . . ";[46]
- the FTC Identity Theft Red Flags Rules, which require most financial institutions and creditors in all sectors to develop and implement a written Identity Theft Prevention Program that includes reasonable policies and procedures for detecting, preventing, and mitigating identity theft in connection with existing accounts or the opening of new accounts;[47]
- the FCC Order addressing the problem of pretexting, which imposes specific authentication requirements on telephone and wireless carriers to protect personal telephone records from unauthorized disclosure;[48]

---

[42] FFIEC Guidance, at p. 2.

[43] See generally, Thomas J. Smedinghoff, "The State of Information Security Law: A Focus on the Key Legal Trends," EDPACS, The EDP Audit , Control, and Security Newsletter (January – February 2008 Vol. XXXVII, Nos. 1–2); http://ssrn.com/abstract=1114246.

[44] GLBA Security Regulations, 12 C.F.R. Part 30 Appendix B, at Part III.C(1)(a) (OCC), 12 C.F.R. Part 208, Appendix D (Federal Reserve System), 12 C.F.R. Part 364, Appendix B (FDIC), 12 C.F.R. Part 568 (Office of Thrift Supervision) and 16 C.F.R. Part 314 (FTC).

[45] HIPAA Security Regulations, 45 C.F.R. § 164.312(d).

[46] *See, e.g.*, Cal. Civil Code § 1798.81.5(b); Mass., Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 CMR 17.04.

[47] 16 C.F.R. Part 681.

[48] *See* FCC Order re Pretexting, 2 April 2007 – In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information IP-Enabled Services, CC Docket No. 96-115, WC Docket No. 04-36, 2 April 2007, at Paragraphs 13-25; available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.pdf

- the Homeland Security Act, which requires "utilizing digital credentials to assure the identity of users and validate their access," and "protecting information and information systems from unauthorized access;"[49]
- Homeland Security Presidential Directive 12, which mandates the development of a Federal standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees), and requires the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems;[50] and
- numerous data protection laws in other countries that also impose similar requirements.[51]

The FTC has also begun to use FTC Act Section 5 to enforce identity management obligations. In the wake of the well-publicized security breach at Choicepoint, the FTC brought a complaint alleging that "ChoicePoint has not employed reasonable and appropriate measures to secure the personal information it collects for sale to its subscribers, including reasonable policies and procedures to: (1) verify or authenticate the identities and qualifications of prospective subscribers; or (2) monitor or otherwise identify unauthorized subscriber activity."[52] Specifically, the FTC alleged that "ChoicePoint failed to detect [false credentials and other misrepresentations] because it had not implemented reasonable procedures to verify or authenticate the identities and qualifications of prospective subscribers."[53]

Similarly, in the March 2009 case of *U.S. v. Rental Research Services, Inc.*,[54] the FTC alleged that a consumer reporting agency failed to employ reasonable and appropriate security policies and procedures to "verify or authenticate the identities and qualifications of prospective subscribers,"[55] and that as a result, it sold at least 318 credit reports to identity thieves. This practice, the FTC asserted, was "an unfair act or practice" in violation of Section 5 of the FTC

---

[49] Homeland Security Act of 2002 § 1001(b), amending 44 U.S.C. § 3532(b)(1)(D), and § 301(b)(1) amending 44 U.S.C. § 3542(b((1) ("'information security' means protecting information and information systems from unauthorized access, ...")

[50] Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors; available at http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm.

[51] *See, e.g.*, Italy, Personal Data Protection Code, Section 34(a) and (b) and Annex B, Sections 1 - 13; Poland, Regulation of April 29, 2004, Section § 5.2 and Attachment A (Basic Security Measures) § II.2; Spain, Royal Decree 1720/2007, Articles 93 and 98 (Basic-level and medium-level security measures);

[52] *United States v. ChoicePoint, Inc.* (Stipulated Final Judgment, FTC File No. 052 3069, N.D. Ga. Jan. 26, 2006), Complaint at Para. 25; available at http://www.ftc.gov/os/caselist/choicepoint/choicepoint.htm.

[53] Id., Complaint at Para. 13.

[54] *U.S. v. Rental Research Services, Inc*., FTC File No. 072 3228, D. Minn. (Stipulated Final Judgment, March 5, 2009), (Settlement of allegations that its lack of reasonable client identification procedures and adequate data security safeguards resulted in the sale of credit reports to identity thieves); available at http://www.ftc.gov/os/caselist/0723228.

[55] *U.S. v. Rental Research Services, Inc*., FTC File No. 072 3228, Complaint, at pars. 28-29, available at http://www.ftc.gov/os/caselist/0723228/090305rrscmpt.pdf.

Act, as well as the FCRA.[56] In addition, the FTC has recently recommended "that Congress consider establishing national consumer authentication standards covering all private sector entities that maintain consumer accounts." These standards, the FTC indicated, "should require private sector entities to create a written program that establishes reasonable procedures to authenticate new or existing customers."[57]

In other cases, courts are finding a common law duty. For example, in *Wolfe v. MBNA America Bank*[58] the court held that, under Tennessee negligence law, where "the injury resulting from the negligent issuance of a credit card is foreseeable and preventable, . . . Defendant has a duty to verify the authenticity and accuracy of a credit account application before issuing a credit card."[59] "[T]his duty to verify" the court held, "requires Defendant to implement reasonable and cost-effective verification methods that can prevent criminals, in some instances, from obtaining a credit card with a stolen identity."[60]

Another example of authentication risk can also be seen in the decision in *Kerr vs. Dillard Store Services, Inc.*, a case involving the enforceability of an electronic signature. There the court refused to attribute an electronic signature to the plaintiff because the authentication process could be easily circumvented, raising legitimate doubts as to who actually signed the electronic record.[61]

(c) Liability Risk

Things that can go wrong in a federated identity management operation typically result from faulty identification, faulty authentication, inadequate security for or misuse of personal data, or failure to follow appropriate procedures. They can lead to two primary harms. First, a Relying Party and/or a Subject may suffer damages when the Relying Party acts (a) in reliance on a false identity credential or identity assertion that it thought was valid (e.g., by granting access to, or entering into an unauthorized transaction with, an imposter), or (b) fails to act in reliance on a valid identity credential that it mistakenly believes to be false. Second, a Subject may suffer damages when (a) his or her personal information is misused or compromised by the Identity Provider or a Relying Party or other third party to whom it has been disclosed, or (b) when the Subject is improperly denied access or the ability to conduct a transaction he is otherwise entitled to do.

---

[56] Id., at para. 29.

[57] Federal Trade Commission Report, "Security in Numbers: SSNs and ID Theft" (FTC, December 2008), at p. 6; available at http://www.ftc.gov/opa/2008/12/ssnreport.shtm (hereinafter **FTC SSN Report**").

[58] *Wolfe v. MBNA America Bank*, 485 F.Supp.2d 874, 882 (W.D. Tenn. 2007).

[59] 485 F.Supp.2d at 882.

[60] Id.

[61] *Kerr vs. Dillard Store Services, Inc*., 2009 U.S. Dist. Lexis 11792 (D. Kan. Feb 17, 2009) (court declined to attribute an electronic signature to an employee because her employer failed to provide adequate security for its intranet passwords).

A primary concern of all participants in any identity federation is determining who will bear the risks associated with these problems and their consequences. For example:

- What is the liability of the Subject for providing false identity information during the identity proofing process, or for failing to protect the password or key necessary to initiate an authentication process? Does the Subject bear the risk of losses due to identity theft facilitated by his or her own negligent actions in the identity management system?
- What is the liability of the Identity Provider for failing to follow proper identification procedures that result in an incorrect identity assertion? For failing to revoke the validity of a token on notice of compromise? For misusing or failing to adequately protect the Subject's personal information?
- What is the liability of the Relying Party for relying on a fraudulent assertion (e.g., in the case of identity theft, especially in a case where it could have determined that the assertion was false)? For misusing or failing to adequately protect the Subject's personal information?

Numerous statutory, common law, and contract theories have been advanced to identify, define, and clarify the source and scope of such potential liabilities.[62] For the Identity Provider, the primary focus from a liability perspective is on the tort of negligent misrepresentation and contract actions for breach of express or implied warranty regarding the accuracy of the information provided. In addition, a potential source of liability for an Identity Provider or Relying Party may arise through the application of provisions contained in privacy and data security legislation and regulations. Yet at the end of the day, the legal risks remain somewhat uncertain.

In many respects, federated identity management is a business model for which the law has not yet had time to adapt. By issuing digital credentials that verify identity, an Identity Provider is, in essence, engaged in the business of an information provider. Moreover, the Identity Provider understands that the information it provides is intended to be relied upon by parties to a commercial transaction. It is this aspect of reliance that is critical. Both the Identity Provider that issues an identity assertion, and the Subject that participates in the process, do so with the intention that it will be used by third parties to verify identity and engage in business transactions. Thus, an Identity Provider risks potential liability to Relying Parties, Subjects, and victims (a class of persons in whose names credentials or identity assertions are improperly issued by the Identity Provider). At the same time, the Relying Party (and often the Subject) is on the front line in bearing the losses and other harms that flow from inaccurate authentication of identity.

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. Without addressing how that liability should be allocated, or who is in the best position to bear the risks, suffice it to

[62] See Thomas J. Smedinghoff, "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://www.wildman.com/resources/articles-pdf/ca-liability-analysis.pdf (hereinafter "**Smedinghoff CA Liability Analysis**").

say that there may be a clear benefit to some legal certainty with respect to this issue. As identity management processes are used for increasingly significant transactions, and the risks to the parties increase accordingly, the benefits to all parties of addressing those risks up front, as well as mitigating those risks (to the extent possible) by requiring performance of specific obligations by each participant role, is significant.

(d) Performance Risk

Finally, for each participant, obtaining the benefits of a federated identity system, and effectively controlling each of the foregoing risks, depends on each of the other roles properly performing certain basic obligations that are fundamental to the concept of federated identity management. The failure of any participant to perform its obligations could lead to substantial harm to others in the federation. In fact, mere concern about the performance of another participant could be fatal to the system. Quite simply, a federated identity model will not function properly, and the various participants will not be able to rely on it for online transactions, unless each participant role has an appropriate degree of confidence or trust that each other participant role will adequately perform certain basic responsibilities.

The fundamental responsibilities of each role include the following:

Subject. The conduct of the Subject can directly affect the validity of the identification and authentication processes. Thus, to ensure accurate and reliable processes, the Subject must:

- Provide accurate information to the Identity Provider during the identification process (e.g., not omit or misrepresent any material fact, or otherwise engage in any identity fraud);
- Prevent the unauthorized use of any token (e.g., a password, PIN, key, etc.) that is issued or registered to the Subject for purposes of the authentication process (e.g., to keep such token confidential and to take reasonable steps to prevent others from gaining access and using it to commit fraud); and
- Notify the Identity Provider if such token is lost or compromised (so that the Identity Provider can take steps to prevent the thief from successfully using it to commit identity fraud).

Identity Provider. The Identity Provider is primarily responsible for the validity and integrity of the identification process and the resulting identity credential, the accuracy of the identity assertions, and the privacy and security of the Subject's personal information in its control. Thus, it must:

- Properly and accurately identify Subjects, and where appropriate, use reasonable procedures to detect omissions or misrepresentations by the Subject;
- Ensure that all identity assertions are accurately based on current valid information that is properly authenticated (e.g., an employer should not issue an identity assertion for a terminated employee);
- Comply with disclosed policies, practices and procedures for the identification and authentication processes (so that Relying Parties can identify assurance levels and

determine the level of trust they should have in the resulting authentication and identity assertions);

- Provide to the Subject a capability to revoke tokens or identity credentials (to limit identity theft opportunities in the event that the Subject's token is compromised or the Subject no longer wants to participate); and
- Protect the privacy and security of Subject's personal information in accordance with disclosed policies, practices and procedures and in accordance with applicable law.

Relying Party. The Relying Party must ensure that its reliance on the identification and authentication processes are reasonable under the circumstances and that its use of the Subject's personal information is appropriate. Specifically, the Relying Party must:

- Properly authenticate credentials and any identity assertions before relying on them (e.g., by analogy, compare a claimant's face to the picture on the driver's license before relying on the data in the license);
- Limit its use and reliance on an identity assertion as appropriate for the circumstances (e.g., credentials issued with a low assurance level, such as a library card, should not be relied upon in situations requiring a very high assurance level, such as access to a sensitive nuclear facility); and
- Protect the privacy and security of the Subject's personal data, and restrict its use of that data in accordance with disclosed policies, practices and procedures and in accordance with applicable law.

Unless each participant has confidence that the other participants will properly perform their obligations, the identity federation is of little value. Thus, there is a need to clearly define the obligations of each role, and to utilize a mechanism (statutory, contractual, and/or technological) to provide some assurance that the participants in each role will perform their obligations, and to provide some remedy if someone does not.

4. Addressing Risks – The Need for a Legal Framework

Depending on their perspective, commentators addressing the legal risks of federated identity management systems put the focus on the privacy concerns of the Subject,[63] the liability concerns of the Identity Provider,[64] or the authentication concerns of the Relying Party.[65] But in

[63] See generally, Landau Article; Privacy Commissioner of Ontario Paper; Thomas Olsen & Tobias Mahler, "Identity Management and Data Protection Law: Risk, Responsibility and Compliance in 'Circles of Trust,'" Computer Law & Security Report Vol. 23(4) (2007), pp. 342-351, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1015006; Liberty Alliance Project, "Circles of Trust: The Implications of EU Data Protection and Privacy Law for Establishing a Legal Framework for Identity Federation," (Feb. 23, 2005); Liberty Alliance Project, "Privacy and Security Best Practices," v.2.0 (November 12, 2003); available at http://www.projectliberty.org/liberty/resource_center/papers/liberty_alliance_privacy_and_security_best_practices (hereinafter "**Liberty Privacy & Security Paper**").

[64] See generally, Paolo Balboni, "Liability of Certification Service Providers Towards Relying Parties and the Need for a Clear System to Enhance the Level of Trust in Electronic Communication," 13 Information & Communications Technology Law No. 3 (2004); Smedinghoff CA Liability Analysis (1998); Michael S. Baum, Federal Certification Authority Liability and Analysis" (U.S. Department of Commerce, 1994).

the final analysis, the benefits of federated identity management won't scale until all of these concerns are adequately addressed in a manner acceptable to all participants, and with adequate enforcement for the legitimate concerns of each. As a recent report noted:

> "Perhaps the one issue that most constrains the effectiveness of today's identification management systems is lack of agreement on how to manage competing demands for identity protection and authentication capabilities with the legitimate need to protect privacy. This is not just a public policy debate but also is infused with pragmatic doubts about the empirical effectiveness of the technologies available such as biometrics, automated access control, and the management practices when data are standardized, federated, and aggregated."[66]

There are many technologies and identity management standards[67] to ensure that personal information moving between organizations is securely transferred and can be read and understood by the systems of all parties. Encryption and digital signature technology, for example, is used to protect the security of the information flows, ensure the integrity of the identity credentials, and to authenticate the Identity Provider to the Relying Party. And technical standards are critical to ensuring the inter-operability of communications across various systems and networks. Without agreement on standards, different networks and systems would be unable to talk to each other and exchange information in a manner that can be understood by either system. But as one commentator has noted regarding the technology: "Ultimately, though, the protection here is legal. A rogue [Relying Party] or Identity Provider is in a position to violate a [Subject's] privacy and *technical protections can only reduce, not eliminate this risk.*"[68]

Some standards have been devised to address, to a certain extent, the legal risks noted above. For example, the Liberty Alliance standards seek to address privacy concerns of the Subject:

> Consumer choice and permission are central to Liberty's vision. The framework of the Liberty Specifications is built upon the presumption that PII will be shared ("attribute sharing") in the context of permissioning, i.e., upon the consent of the [Subject] and in accordance with the usages expressed by the [Subject]. Such attribute sharing should be predicated upon not only a prior agreement between the Liberty-Enabled Providers, but also upon providing notice to the [Subject]and

---

[65] See generally, FTC SSN Report, FFIEC Guidelines, Transition Study Group Report, OSTP Report, _____.

[66] Transition Study Group Report, at p. 4.

[67] See, e.g., Liberty Alliance specifications at http://www.projectliberty.org/liberty/specifications__1; National Institute of Standards and Technology, Federal Information Processing Standards Publication FIPS Pub. 201-1 "Personal Identity Verification (PIV) of Federal Employees and Contractors" (March 2006); CA/Browser Forum, "Guidelines for the Issuance and Management of Extended Validation Certificates" (2008) at Part F; available at http://cabforum.org/EV_Certificate_Guidelines_V11.pdf.

[68] Landau Article, Section 3.2 (emphasis added).

> obtaining the [Subject]'s consent. The Liberty Specifications allow for recording both the notice and consent in an auditable fashion.[69]

But as the Privacy Commissioner of Ontario has noted, "The majority of users, however, are neither capable of nor interested in micromanaging the ecosystem."[70]

At the end of the day, technology and standards do not, by themselves, adequately address the primary legal risks of a federated identity management system noted above. What the parties do when creating or using identity information is generally outside the scope of those standards. Thus, the privacy risks (to the Subject), the liability risks (to the Identity Provider), and the authentication risks (to the Relying Party) are largely determined by the authenticity, reliability, and security of the personal information stored at either end (i.e., with either the Identity Provider or the Relying Party), and perhaps most importantly, by the conduct of the parties with respect to it.

For example, some have argued that, in order to protect the privacy of the Subject, the information disclosed by the Identity Provider to the relying Party should be both minimal and unlinkable:

> First, the information presented should be *minimal* – that is, only exactly what the Relying Party needs to know about the user should be revealed by the agent, and no more. For example, as mentioned above, if the Relying Party needs to know that I am over 21, then that is what should be revealed, not my date of birth. Or if the Relying Party needs to know that I am a member of some club (customers of a particular bank, for example) then what should be disclosed is just that fact, not *which* member of the club I am.
>
> Second, presentations of information should be *unlinkable*. That is, if I go to a website today and prove I'm over 21, and then go to the same website tomorrow and prove it again, the website should not be able to link those two events together to know it was the same user that made the two proofs. Unlinkability should also be in effect when proving different information, or going to different Relying Parties. This feature prevents the Relying Party (or a group of parties) from gathering information a piece at a time until my entire profile has been revealed and is then available on each future interaction, regardless of what I intend to disclose at that time.[71]

---

[69] Liberty Privacy & Security Paper, at p. 9.

[70] Privacy Commissioner of Ontario Paper, at p. 7.

[71] Mary Rundle and Ben Laurie, "Identity Management as a Cybersecurity Case Study," The Berkman Center for Internet & Society, Research Publication No. 2006-01 (September 2005), at p. 7; available at http://cyber.law.harvard.edu/node/418 and http://ssrn.com/abstract=881107. See also, Landau Article, Section 2.1, which makes essentially the same suggestion: "Identity-management systems should use the principle of minimal disclosure, and should be able to engage where no PII is exchanged. Federation allows information to be distributed with each SP receiving exactly the information needed for its role—though many service providers may have to adjust to the concept (since they will no longer receive PII). To reduce liability, many organizations will choose to limit the PII they hold (and then protect the PII they hold in various ways: protected databases, strict access rules, careful auditing procedures, as well as some PETs, including those described below). Federated systems allow them to do so, and there have been several approaches to this — both theoretical and within deployed systems."

While these are important principles, and the technology and the standards used can certainly help to facilitate these objectives, at the end of the day, achieving these goals is up to the performance of the parties. In other words, they are subject to performance risk.

Thus, technology and standards may help control these risks somewhat. But as one commentator has noted, they typically "address only the *exchange* of information. Whatever the parties do to produce or consume the information that was exchanged is outside the scope of these protocols."[72] Thus (with respect to one of these risks, privacy): "We . . . contend that the privacy solutions for identity management should be a combination of technical and non-technical measures, capable of adjusting to different legal, regulatory and liability contexts."[73]

In other words, some sort of a legal framework is required in order to govern the conduct of the participants in a federated system and address the legal risks noted above. Such a framework should allow for regulation of the behavior of the participants in the federated identity process, and provide a basis for enforcement (e.g., a legal remedy) in the case of a failure to comply.

The comments of the Privacy Commissioner of Ontario, made in the context of addressing the privacy risk, illustrate this need:

> Privacy and trustworthiness may be more difficult to establish within a federation of multiple enterprises than within a single enterprise. In a lone enterprise, there is typically a common policy framework, technology implementation and user base; many tools exist, such as Privacy Impact Assessments, with which a company can demonstrate and delineate its data protection efforts. Across multiple enterprises, however, there will likely be many different policies, deployed technologies and types of users, all of which need to be both interoperable and consistent in the protections provided for shared data. Strong privacy measures undertaken by a single enterprise become meaningless if its data-trading partners do not have compatible measures; the policies and technologies of *all* federation members must satisfy the requirements of the trusting party.[74]

5. Models for a Legal Framework

An effective legal framework for a federated identity management system must balance the competing needs and goals of the primary participant roles, i.e., Subjects, Identity Providers, and Relying Parties. Moreover, it must achieve five primary goals:

---

[72] Landau Article, Section 3.2 (emphasis in original)

[73] Landau Article, Section 2.4.

[74] Privacy Commissioner of Ontario Paper, at p. 7.

- It must clearly define the rights and responsibilities of all of the participant roles so that the process works properly, effectively, and reliably to establish the required level of trust;

- It must operate in compliance with all existing laws governing the privacy and security of personal information, and requirements for the authentication of individuals in online transactions;

- It must fairly allocate among the participant roles the key legal risks noted above;

- It must provide some basis of ensuring, before the fact, that all roles (particularly the Identity Providers) have the necessary processes and technologies in place to properly perform their obligations, and are currently implementing those in an appropriate manner (e.g., via an appropriate audit);

- It must provide a realistic enforcement mechanism and remedy in the event that a participant fails to act in the required manner (e.g., terminate its participation, provide for the recovery of damages, etc.).

There are a variety of approaches to establishing such a legal framework, as discussed below. It appears, however, that a binding contractual framework agreed upon by the parties will work best.

(a) Legislative/Regulatory Approaches

One obvious solution to the need for a legal framework is legislation and regulation. In theory, the law could be fashioned so as to provide the requisite rules to govern a federated identity model. This would provide the advantage of legal certainty for the participants through a series of legal requirements that would specify the rights and responsibilities of the participants and (at least in theory) reflect a socially-acceptable allocation of the risks among them.

This approach was initially tried in the mid 1990s in an attempt to provide a set of rules and regulations for a form of federated identity known as a public key infrastructure, or PKI. Examples of attempts at comprehensive laws include the digital signature laws enacted in Utah, Washington, Missouri, and Minnesota in the U.S.,[75] and similar laws enacted in Germany, Italy, Malaysia, Columbia, and other countries.[76] Examples of more limited statutory approaches to these issues include provisions found in the EU Electronic Signatures Directive,[77] and the UNCITRAL Model Law on Electronic Signatures (which has been incorporated into the law of several countries).[78]

---

[75] *See* Minn. Stat. Ann. § 325K.20 (West 1998); Mo. Ann. Stat. § 28.657 (West 1999); N.H. Rev. Stat. Ann. § 294-D:4 (1999); Utah Code Ann. §§ 46-3-101 to 46-3-504 (1998); Wash. Rev.. Code Ann. § 19.34.900 (West 1998).

[76] See, generally, Stephen Mason, ELECTRONIC SIGNATURES IN LAW, 2d Ed. (Tottel Publishing, 2007)

[77] See, e.g., EU Electronic Signatures Directive, Articles 6 – 8 and Annexes I and II.

[78] See United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Signatures 2001, Articles 8 – 12, available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html

Although some of these laws remain (and thus they must be addressed in the jurisdictions where they exist), the approach has now been largely rejected (particularly in the U.S. and to a lesser extent in the EU), in favor of a more technology-neutral approach in law, so as to promote (rather than stifle) experimentation and innovation. Practical experience also suggested that this approach was not particularly workable, especially as the technology and approaches to federated identity evolved and matured.

Nonetheless, participants in a federated identity model still need to recognize that there are numerous laws and regulations which, while often not specifically focused on identity management, may have a significant regulatory impact (and in some cases, will impose mandatory requirements). Foremost among these are the various domestic and international laws regulating the privacy and security of the personal information that is collected and shared as part of any identity management process, the developing body of law governing the duty to authenticate as noted above, and the common law of negligent misrepresentation which may govern the liability of the Identity Provider for incorrect identity credentials and identity assertions.

In the EU, for example, the Electronic Signatures Directive mandates that member states regulate the collection of personal data about Subjects by certain Identity Providers (called certification service providers).[79] And transfer of that data across country borders, whether for identification or identity assertion purposes, will also raise issues under the EU Data Protection Directive and implementing country laws. In the U.S., state security laws governing personal information will also be a key factor. And in regulated industries, compliance with privacy laws such as GLB and HIPAA will be important.

But in the final analysis, many issues, including most of the responsibilities and concerns of the various participant roles noted above, remain open and unresolved by any law. As a result, common law will fill in most of the gaps,[80] unless the participants address the issues by contract or binding standards.

(b) Unilateral Assertion Models

Another early approach to the issue involved what might be referred to as a unilateral assertion. That is, an Identity Provider simply established its own rules and standards, by publicly declaring the manner in which it operates, the rules it agrees to follow, and the liability (if any) that it will accept. This is based on the premise that by publicly declaring its rules, Subjects and Relying Parties who participated with notice would be bound by the limitations of the self-declared standard. An example of this approach can be seen in the Certification Practices Statement issued by VeriSign with respect to the digital certificates that it issues.[81]

---

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

[80] See, e.g., Smedinghoff CA Liability Analysis.

[81] See VeriSign Certification Practice Statement (CPS), available at http://www.verisign.com/repository/CPS

While there has been some analysis of the enforceability of this approach,[82] it has not really been tested. Moreover, as it is designed primarily to address the liability risk of the Identity Provider, and to the extent it addresses privacy risk and/or authentication risk, its focus is likely to be more from the perspective of the entity issuing the document.

(c) Contractual Models

An increasingly common approach to providing the rules that will govern the parties and the allocation of risk among them is to bind the participants to a pre-defined set of rules and legal obligations by contract. Such contract is, of course, subject to the binding requirements of applicable laws governing the privacy, authentication, and liability risks.

The Liberty Alliance, for example, recommends that the participants establish a contractual infrastructure that it refers to as a legally binding "Circle of Trust."[83] This allows the parties to agree, in advance, on all of the obligations, rules, and remedies that will govern their relationship. Examples of federated identity management models that include such comprehensive contractual models include IdenTrust,[84] which provides federated identity solutions in the financial sector, the SAFE-BioPharma Association,[85] which provides federated identity solutions in the pharmaceutical sector, and Certipath,[86] which provides federated identity solutions in the aerospace sector.

The Liberty Alliance defines several contractual models,[87] but they focus on ways to organize the relationships, not on how to address the performance, privacy, authentication, and liability risks. Addressing those risks requires detailed contractual provisions that define the rights, responsibilities, and obligations of the various roles, as well as enforcement mechanisms that are designed (ideally) to ensure proper performance before it is required, and to impose liability (or other punishment) after failures occur.

The rights, responsibilities, and obligations of the various roles might be set forth in the contract itself, or alternatively might be defined as a separate set of standards maintained by a standards body. In such a case, the participants in the identity federation might agree (contractually) that such standards will govern their rights and responsibilities in the identity federation, and might require an independent audit for verification. Alternatively, Identity

---

[82] See, e.g., Smedinghoff CA Liability Analysis.

[83] See, e.g., The Liberty Alliance Project, "Liberty Alliance Contractual Framework Outline for Circles of Trust," available at http://www.projectliberty.org/liberty/files/whitepapers/liberty_alliance_contractual_framework_outline_for_circles_of_trust (hereinafter "**Liberty Circles of Trust Paper**")

[84] http://www.identrust.com

[85] http://www.safe-biopharma.org

[86] http://www.certipath.com

[87] The Liberty Alliance defines three contractual models, which it refers to as the Collaborative Model, the Consortium Model, and the Centralized Model. See Liberty Circles of Trust Paper. Other organizations (such as Certipath) have defined other models.

Providers might opt-in to those standards, such as by publicly declaring their willingness to be bound by them, and submitting to an independent audit to verify their compliance as a condition of participating. The theory is that other parties that rely on identity assertions are on notice as to the rules, and by their reliance on the identity assertions are bound thereby. An example of this approach is the EV SSL Certificate Guidelines and the WebTrust audit requirements specified by the CA/Browser Forum for the issuance and use of Extended Validation SSL certificates to identify website operators.[88]

Each of the foregoing approaches has positive and negative attributes, and raises numerous complexities, but all are essentially untested by any court. Yet, without some type of a legal framework to address issues such as those noted above, a federated identity model will likely not scale. Otherwise, at least in the case of economically significant transactions, the risks to each of the parties of such unresolved issues may be too great to justify reliance on the federated process. Providing a legal mechanism to address these questions, and others like them is key to establishing a viable federated identity management infrastructure.

* * *

The American Bar Association, through the Federated Identity Management Task Force of the Cyberspace Committee of its Business Law Section,[89] has recently undertaken a project to develop a model for the contract terms that would define such a federated identity management framework. The Task Force is working in cooperation with the Liberty Alliance,[90] a federated identity management standards developing organization. Persons interested in participating should contact one of the Task Force co-chairs, Thomas J. Smedinghoff (smedinghoff@wildman.com), R. David Whitaker (david.whitaker@wellsfargo.com), or Jane K. Winn (jkwinn1@u.washington.edu).

[88] See CA/Browser Forum website at http://www.cabforum.org.

[89] http://www.abanet.org/dch/committee.cfm?com=CL320041

[90] http://www.projectliberty.org

Glossary

Attribute. Personal information concerning a specific category or characteristics of a given identity, such as name, address, age, gender, title, salary, health, net worth, driver's license number, Social Security number, etc.

Authentication. The process of establishing or confirming that someone is who they claim to be.

Authenticator. Something (usually uniquely in the possession of a person) that is used to determine authenticity; usually an object, an item of knowledge, or some characteristic of its possessor that is used to tie a person to an identity credential (such as by demonstrating that such person has possession of the authenticator). Also called a token. A password functions as an authenticator.

Authenticity. The property that data originated from its purported source

Authorization - A process of controlling access to information or resources only to those specifically permitted to use them. The actions that an authenticated person or entity is permitted as a result of the authentication.

Claim. An assertion made by a person with respect to one or more identity attributes of a Subject, which assertion typically is disputed or in doubt.

Credential – A digital document that binds a person's identity (and optionally, additional attributes) to a token possessed and controlled by a person. Data that is used to establish the claimed attributes or identity of a person or an entity. Paper credentials are documents that attest to the identity or other attributes of an individual or entity called the Subject of the credentials. Some common paper credentials include passports, birth certificates, driver's licenses, and employee identity cards.

Enrolment – The process by which organizations verify an individual's identity claims before issuing digital credentials.

Identification. The process of verifying and associating attributes with a particular person designated by an identifier.

Identifier. Something that points to an individual, such as a name, a serial number, or some other pointer to the party being identified. Since a person's legal name is not necessarily unique, the identifier of a person must include sufficient additional information (for example an address, or some unique identifier such as an employee or account number) to make it unique. For a typical login account, the User ID is the identifier and the password is the authenticator.

Identity. A unique name of an individual person (an identifier), and any associated attributes; the set of the properties of a person that allows the person to be distinguished from other persons.

Identity Assertion – An electronic record sent by an Identity Provider to a Relying Party that contains the Subject's identifier (e.g., name, account number, etc.), authentication status, and identity attributes. The attributes are typically personal information about the Subject relevant to the transaction that is required by the Relying Party.

Identity Proofing. The process by which an Identity provider validates sufficient information to uniquely identify a person.

Identity Provider. An entity that creates, maintains, and manages identity information for Subjects. It authenticates and vouches for the Subject to Relying Parties.

Relying Party. An entity that provides services to a Subject, or otherwise has a need to authenticate the identity of the Subject, and that relies on an Identity Provider for identity and authentication of the Subject, typically to process a transaction or grant access to information or a system. The entity or person 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.

Role. A type of participant in a federated identity system, such as a Subject, Identity Provider, or Relying Party. Note that each such role does not necessarily represent a different entity. For example, with respect to the identification of its employees, an employer may function as both an Identity Provider and a Relying Party.

Strength. The technical and procedural basis on which to believe that a particular process or data attribute is accurate.

Subject. The person that is identified in a particular credential and that can be authenticated and vouched for by an Identity Provider

Token. Something that a person possess and controls (either a unique physical object or secret data or information) that is used to authenticate his or her identity (such as a secret password, PIN, cryptographic key, ATM card, USB token, etc.). Tokens are physical devices or electronic records designed for use in authentication systems and/or to hold authenticating information. These include smart cards and ATM cards as well as digital certificates. Also called an authenticator.

List of Papers and Reports
Cited in Footnotes

1. Peter Alterman, "On the Reliability of Authentication of Identity;" available at http://www.cio.gov/fpkipa/documents/ReliabilityAuthenticationIdentity.pdf

2. European Commission, "Action Plan on e-signatures and e-identification to facilitate the provision of crossborder public services in the Single Market," COM(2008) 798 final (28 November 2008); available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0798:FIN:EN:PDF

3. **FFIEC Guidance:** Federal Financial Institutions Examination Council ("FFIEC"), "Authentication in an Internet Banking Environment," October 12, 2005; available at http://www.ffiec.gov/pdf/authentication_guidance.pdf

4. Jacques R. Francoeur and Edward Chase, "Digital Signature Assurance & the Digital Chain of Evidence," Version 1.0, January 2009; [copy on file with author]

5. **FTC SSN Report:** Federal Trade Commission Report, "Security in Numbers: SSNs and ID Theft" (FTC, December 2008); available at http://www.ftc.gov/opa/2008/12/ssnreport.shtm

6. Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors; available at http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm

7. **Landau Article:** Susan Landau, Hubert Le Van Gong, and Robin Wilton, "Achieving Privacy in a Federated Identity Management System,**"** (2009); available at http://research.sun.com/people/slandau/Achieving_Privacy.pdf

8. **Liberty Privacy & Security Paper:** Liberty Alliance Project, "Privacy and Security Best Practices," v.2.0 (November 12, 2003); available at http://www.projectliberty.org/liberty/resource_center/papers/liberty_alliance_privacy_and_security_best_practices

9. **Liberty Circles of Trust Paper:** The Liberty Alliance Project, "Liberty Alliance Contractual Framework Outline for Circles of Trust," available at http://www.projectliberty.org/liberty/files/whitepapers/liberty_alliance_contractual_framework_outline_for_circles_of_trust

10. **Liberty Identity Assurance Framework:** Liberty Alliance Project, Liberty Identity Assurance Framework, Version 1.1 (2008); available at http://www.projectliberty.org/resource_center/specifications/liberty_alliance_identity_assurance_framework_iaf_1_1_specification_and_associated_read_me_first_1_0_white_paper

11. **NIST Special Publication 800-63:** National Institute of Standards and Technology, "Electronic Authentication Guideline," Special Publication No. 800-63, Version 1.0.2, (April, 2006); available at http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

12. Organisation for Economic Co-operation and Development (OECD) Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication, June 2007; available at http://www.oecd.org/dataoecd/32/45/38921342.pdf

13. **OECD Report**: OECD Working Party on Information Security and Privacy, The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers**,** DSTI/ICCP/REG(2008)10/FINAL, (June 11, 2009); available at http://www.oecd.org/dataoecd/55/48/43091476.pdf

14. Thomas Olsen & Tobias Mahler, "Identity Management and Data Protection Law: Risk, Responsibility and Compliance in 'Circles of Trust,'" Computer Law & Security Report Vol. 23(4) (2007); available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1015006

15. **OMB Memo M-04-04:** Office of Management and Budget, **"**E-Authentication Guidance for Federal Agencies," OMB Memo M-04-04, (December 16, 2003); available at http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

16. **OSTP Report:** Office of Science and Technology Policy (OSTP), National Science and Technology Council (NSTC), Subcommittee on Biometrics and Identity Management, "Identity Management Task Force Report 2008," (September 2008); available at http://www.ostp.gov/galleries/NSTC%20Reports/IdMReport%20Final.pdf

17. **Privacy Commissioner of Ontario Paper:** Information and Privacy Commissioner of Ontario, "The New Federated Privacy Impact Assessment (F-PIA): Building Privacy and Trust-enabled Federation" (January, 2009); available at http://www.ipc.on.ca/images/Resources/F-PIA_2.pdf

18. Mary Rundle and Ben Laurie, "Identity Management as a Cybersecurity Case Study," The Berkman Center for Internet & Society, Research Publication No. 2006-01 (September 2005); available at http://cyber.law.harvard.edu/node/418 and http://ssrn.com/abstract=881107

19. **Smedinghoff CA Liability Analysis:** Thomas J. Smedinghoff, "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://www.wildman.com/resources/articles-pdf/ca-liability-analysis.pdf

20. Thomas J. Smedinghoff, "The State of Information Security Law: A Focus on the Key Legal Trends," EDPACS, The EDP Audit , Control, and Security Newsletter (January – February 2008 Vol. XXXVII, Nos. 1–2); available at http://ssrn.com/abstract=1114246

21. **Transition Study Group Report**: Industry Advisory Council Transition Study Group, "Identity and Access Management," (December 9, 2008); available at www.actgov.org/knowledgebank/studies/Documents/Transition%20Study%20Group%20Papers/Identity%20and%20Access%20Management,%20IAC,%2012-9-2008.pdf