SOLVING THE LEGAL CHALLENGES IN VERIFYING ONLINE IDENTITY

By Thomas J. Smedinghoff

In this age of phishing, hacking, identity fraud, and other forms of cybercrime, answering two simple questions—"Who are you?" and "How can you prove it?"—is fast becoming a critical requirement for online business activities.

In fact, this issue of online identity was elevated to a key priority by the White House in April 2011 when it released its *National Strategy for Trusted Identities in Cyberspace* (*"National Strategy"*).[1] Through this document, the administration began the process of tackling the difficult problem of facilitating a trustworthy and interoperable online identity management capability.

Solving this identity management challenge has become quite complex as the increasing need for cross-organization collaboration, concerns about security, and the problem of user password management suggest that the traditional company- or vendor-issued username and password approach is no longer adequate. As a consequence, various forms of *federated* identity management, where a third-party identity provider plays a key role, are rapidly emerging as a preferred approach.

Critical to making it work, however, is the requirement for an appropriate, and typically voluntary, legal framework that will define the rights and responsibilities of the parties, allocate risk, and provide a basis for enforcement.

Understanding the legal challenges of identity management, its impact potential on business, and the significance of the US *National Strategy*, begins with understanding the principles of identity management, and its role in everyday online business activity.

Thomas J. Smedinghoff is a partner in the Privacy & Data Protection Group in the Chicago office of Edwards Wildman Palmer LLP. He was the 1999–2000 Chair of the Section of Science & Technology Law and is currently Chair of the Identity Management Legal Task Force of the Section of Business Law's Cyberspace Committee. He can be reached at tsmedinghoff@edwardswildman.com.

Identity Management Basics

Although the term *identity management* is relatively 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, and employee ID cards are all components of what might be referred to as identity management systems—i.e., they are credentials issued by an entity for the purpose of identifying individuals, and they are used by such individuals to validate their identity. A key element is that the use of these identity credentials is not limited to transactions with the entities that issued them. Rather, they are often accepted by third parties (such as airport security, or a bartender) when proof of certain aspects of one's identity is required.

Although there are many different approaches to identity management, it essentially involves two fundamental processes: (1) the process of verifying certain identity attributes about a person and issuing an identity credential to reflect those attributes (identification); and (2) the process of later verifying that a particular person presenting that credential and claiming to be that previously identified person is, in fact, such person (authentication).

The *identification* process is designed to answer the question "Who are you?" Performed by someone filling the role of an *identity provider*, it involves associating one or more identifying attributes (e.g., name, address, height, birth date, SSN, employer, membership number) with a person in order to identify and define that individual to the level sufficient for the contemplated purpose. Sometimes called *identity proofing*, this process is usually a one-time event. It typically involves the collection by an identity provider of personal information about the person to be identified (referred to as the *subject*) and often relies on a patchwork of government-issued documents, from birth certificates and Social Security cards to driver's licenses and passports.

At the end of the identification process, the subject's identity is typically represented by data in a paper or electronic document issued by the identity provider and referred to as an identity *credential*. A credential is the verified attribute data relating to the identity of a specific person. In the physical world identity credentials include driver's licenses, passports, and employee identification cards. In the online world, the identity credential might be as simple as a user ID or as complex as a cryptographically based digital certificate that might be stored on a computer, cell phone, smart card, ATM card, flash drive, or similar device.

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

This typically requires a process to tie the person to the credential. If the credential is a driver's license, this association is typically done by comparing the picture on the license to the person presenting it. With an online user ID, the association is established by use of a secret PIN or password which (in theory) is known only to the person to whom the user ID was issued.

Once a person is successfully authenticated, the relying party uses an *authorization* process to determine what rights and privileges are accorded to such person—e.g., whether such person should be granted access to a website, a database, a bar, an airport boarding area, etc. This process addresses the question "What can you

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.

A familiar offline example of this type of identity management process is the way we currently issue and use driver's licenses. Issued by the department of motor vehicles in each of the various states, they are used by various relying parties to verify attributes about the identity of the subject, such as by a TSA agent to verify the name of a person seeking to enter an airport boarding area, or by a bartender to verify the age of a person ordering a drink.

An online example is the typical ATM transaction whereby an individual with an account at Bank A uses the identity credential issued by his bank (the ATM card) to obtain cash from an ATM machine operated by Bank B (with whom he has no relationship). 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).

Building an Online Identity System

The critical importance of online identity management in facilitating trustworthy e-commerce and ensuring national security is now well recognized. Several governments, intergovernmental forums, and private groups are already actively working to address the applicable technical and legal issues. A recently released survey by the OECD[2] reviews the national strategies of 18 countries actively pursuing online identity management. Intergovernmental forums working on identity management include the International Telecommunications Union (ITU), the OECD, and the International Standards Organization (ISO). Private sector groups working on identity issues include the Open Identity Exchange (OIX),[3] the Kantara Initiative,[4] the Open ID Foundation,[5] the Information Card Foundation,[6] and the Organization for the Advancement of Structured Information Standards (OASIS).[7]

With its *National Strategy*, the United States seeks to chart a course for the public and private sectors to collaborate in an effort to address the problem of online identity management. Unlike many EU countries, however, the *National Strategy* makes clear that it "does not advocate for the establishment of a national identification card."[8] Instead, it seeks to establish a voluntary interoperable identity ecosystem where individuals have the choice of obtaining and using different credentials from a variety of different private sector identity providers.[9]

The vision of the *National Strategy* is that businesses and government agencies will be able to rely on an identification process performed, and identity information provided, by any one of several third-party identity providers—a so-called *federated* model. In other words, identity information would be portable across different systems and entities. This would, for example, allow individuals and businesses to use an identity credential of their choosing to conduct online transactions with numerous enterprises, just as an individual might use a driver's license for a variety of different offline transactions, such as buying alcohol, gaining admission to an airport boarding area, or opening a bank account.

Building private sector identity trust frameworks for interoperable online identity systems is the challenge that lies ahead.

Achieving this goal requires building an identity system that is secure (e.g., protected against falsification or hacking); where identity credentials will be interoperable (so that one credential can be used with numerous relying parties); that is privacy-enhancing (so that individuals will be in control of the use of their personal information); where participation is voluntary; and that is cost-effective for relying parties and easy to use for individuals.

The Need for a Trust Framework

Making such an identity system work in an open online environment requires not only the implementation of appropriate software and communication technologies, but also adherence by all participants (e.g., subjects, identity providers, and relying parties) to a common set of technical standards, operational requirements, and legal rules. Achieving that goal requires building what is often referred to as an identity *trust framework*.

An identity trust framework is a governance structure that consists of two general categories of components: (i) the technical specifications and operational rules and requirements necessary to make the system functional and trustworthy; and (ii) the legal rules that define the rights and legal obligations of the parties and facilitate enforcement where necessary.

The *technical and operational specifications* of an identity trust framework define the requirements for the proper operation of the identity system (i.e., so that it works), define the roles and operational responsibilities of the participants, and provide adequate assurance regarding the accuracy, integrity, privacy, and security of its processes and data (i.e., so that the various parties are willing to participate; so it is trustworthy).

The *legal rules* for an identity trust framework consist of both existing statutes and regulations (i.e., publicly created law), and agreements between or among the participants (i.e., privately created law). They regulate the content of the technical and operational specifications; make them legally binding on and enforceable against the participants; define and govern the legal rights, responsibilities, and liabilities of the participants of the identity system; clarify the legal risks parties assume by participating in the trust framework (e.g., warranties, liability for losses, risks to their personal data); and provide remedies in the event of disputes among the parties, including methods of dispute resolution, enforcement mechanisms, termination rights, and measures of damages, penalties, and other forms of liability.

At its essence, an identity trust framework is much like the trust frameworks (aka system rules) used for the payment portion of an online transaction. For credit card transactions, a credit card trust framework provides the specifications and rules applicable to the participants in an online credit transaction and subsequent processing.[10] Likewise, an electronic funds transfer trust framework provides the specifications and rules applicable to the participants whenever electronic funds transfers (e.g., ACH transfers) are used as the method of payment in an online transaction.[11]

Trust frameworks typically regulate the conduct of the participants in an online transaction, including consumers. The credit card trust framework, for example, regulates the responsibilities of issuers, processors, relying party merchants, and individual cardholders. Likewise, the ACH trust framework regulates the responsibilities of all of the banks in the payment process, as well as, to a limited extent, the consumers or other payers involved.

Although the need for an identity trust framework containing appropriate legal rules is generally acknowledged, developing it is uncharted territory. There are numerous legal issues and legal barriers that must be identified and addressed. The *National Strategy* offers few clues as to how this will be accomplished, but it does raise the two major categories of legal issues that have generated the most concern, and that have generally been perceived as major barriers—privacy and liability.

Addressing the Privacy Issues

By its nature, any form of identity management typically involves the collection (by an identity provider) and disclosure (to a relying party) of some personal information about a subject. To benefit from participation in an 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 information identity providers collect about them during the identification process and disclose to relying parties during the authentication process 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, a foundational issue for any identity system trust framework is protecting the privacy of personal information. This may involve addressing questions such as: What information may be collected by the identity provider? How much information may be disclosed to relying parties? How securely must the data be handled by the parties? What limits are imposed on use of the information by the identity provider and relying parties? Presumably these questions can be addressed by contractual rules or legislation.

In the United States, there is generally little or no law to govern the privacy of this data (except for law in the financial and health care sectors, and laws regulating certain types of data, such as Social Security numbers, credit card data, etc.). But the *National Strategy* views the privacy issue as a key one, particularly from the perspective of incentivizing individuals to participate. It argues that identity trust frameworks "must offer individuals better means of protecting their privacy by establishing clear rules and guidelines . . . [that] address not only the circumstances under which a service provider or relying party may share information but also the kinds of information that they may collect and how that information is used."[12] To accomplish this, the *National Strategy* contemplates new privacy requirements, based on the Fair Information Practice Principles.[13]

The *National Strategy* seeks to further address the privacy issue, by advocating for what it refers to as a user-centric approach. Under a user-centric approach, subjects control the use of their identity credentials, rather than identity providers or relying parties. That is, like a traditional paper-based transaction, the user would choose which identity credential to provide for a given transaction, and thus be able to exert some level of control over the personal information disclosed.[14]

Resolving these privacy issues may well be a contentious process. Moreover, the user-centric approach might not be practical in all cases, and even where implemented, may not give the subjects complete control of the use of their data. Nonetheless, there is little doubt that privacy is a major issue that must be addressed if secure, interoperable online identity management capabilities are to become a reality.

Addressing the Liability Issues

The other primary legal concern of importance to the participants in any identity ecosystem is determining who will bear the risks associated with faulty identification or authentication, failure of technology, and other problems or failures of performance that might lead to unauthorized access through identity fraud or mistake. These concerns about liability include questions such as:

- What is the liability of the subject for failing to protect the password or key necessary to activate an identity credential and 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 credential 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 fraudulent identity information (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.[15] Yet at the end of the day, the legal risks remain ill defined and uncertain.

All participants in a federated identity system have an interest in fairly allocating, in advance, the risk of liability that flows from participation in the process, as well as mitigating those risks to the extent possible. Without addressing how that liability should be allocated, or who is in the best position to bear the risks, suffice it to say that the existing legal uncertainties with respect to this issue are a major barrier to the implementation of a trustworthy identity system. 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.

The US *National Strategy* recognizes that concerns around liability represent a key barrier to private sector adoption of interoperable identity management solutions. It anticipates that liability issues will be best addressed by contractual agreement among the participants, but also recognizes that legislation may be ultimately necessary to address some of those concerns. This is, in fact, the approach we see with the credit card and electronic payment system models. Although both models contain extensive contract-based rules regarding liability allocation, those rules are also supplemented by regulation with respect to consumer liability.

Path Forward

Building private sector identity trust frameworks for interoperable online identity systems is the challenge that lies ahead. As with the credit card and electronic payment systems, the trust framework for online identity management systems are likely to be primarily contract-based, but subject to appropriate legislation with respect to certain issues, such as the protection of consumers.

There are some examples of private sector identity trust frameworks. These are primarily focused on high-risk transactions, and include IdenTrust[16] which has established an identity trust framework for the financial sector, the SAFE-BioPharma Association,[17] which has established an identity trust framework for the pharmaceutical sector, and CertiPath,[18] which has established an identity trust framework for the aerospace and defense sector.

The task ahead will be to develop open and interoperable identity trust frameworks available to everyone. ◆

Endnotes

1. *National Strategy for Trusted Identities in Cyberspace*, Apr. 15, 2011, *available at* www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf ("*National Strategy*").

2. Laurent Bernat, *National Strategies and Policies for Digital Identity Management in OECD Countries*, OECD Digital Economy Papers, No. 177, OECD Publishing. doi: 10.1787/5kgdzvn5rfs2-en; available at www.oecd-ilibrary.org/content/workingpaper/5kgdzvn5rfs2-en.

3. www.openidentityexchange.com.

4. http://kantarainitiative.org/, formerly known as the Liberty Alliance, www.projectliberty.org.

5. http://openid.net/foundation.

6. http://informationcard.net/foundation.

7. www.oasis-open.org/home/index.php.

8. *National Strategy*, at 8.

9. *National Strategy*, at 3, 12.

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

11. The electronic funds transfer trust framework includes the specifications and rules for EFT transactions (e.g., the Operating Rules and Guidelines of NACHA—The Electronic Payments Association, available for a fee at www.nacha.org) that are made binding on the processing banks and the merchants, as well as the contracts between the merchants and the individual payers. It is supplemented by laws and regulations that govern electronic funds transfers, such as the electronic Funds Transfer Act and Regulation E.

12. *National Strategy* at 29.

13. See *National Strategy*, at 12, 29, and Appendix A.

14. For a discussion of this approach, see Heather West, *Issues for Responsible User-Centric Identity*, Center for Democracy & Technology, (Nov. 2009, Version 1.0); available at www.cdt.org/paper/issues-responsible-user-centric-identity.

15. See *Certification Authority Liability Analysis* (study for the American Bankers Association, discussing potential liability risks of an identity provider operating as a certification authority); *available at* www.wildman.com/resources/articles-pdf/ca-liability-analysis.pdf.

16. www.identrust.com.

17. www.safe-biopharma.org.

18. www.certipath.com.