BNA, INC.

PRIVACY & SECURITY LAW

REPORT

BNA Employee-Owned Since 1947

Building an Online Identity Legal Framework: The Proposed National Strategy

By Thomas J. Smedinghoff

Declaring that "the Federal Government must address the recent and alarming rise in online fraud, identity theft, and misuse of information online," the White House released for public comment its draft *National Strategy for Trusted Identities in Cyberspace*[1] June 25. Through this document, the Administration has begun the process of tackling the difficult issue of facilitating a trustworthy and interoperable online identity management capability.

Thomas J. Smedinghoff is a partner in the Privacy, Data Security and Information Law Practice at the law firm of Wildman Harrold in Chicago. He is Co-Chair of the Federated Identity Management Legal Task Force of the American Bar Association Section of Business Law and is on the advisory board for BNA's Privacy & Security Law Report. Smedinghoff, who provided input to the drafting process for the National Strategy for Trusted Identities in Cyberspace, can be reached at smedinghoff@wildman.com.

In essence, after many years of both public and private efforts to address the problem of online identity, the White House has effectively concluded that secure, interoperable, and easy-to-use online identity management capabilities won't become a reality until the federal government provides the incentives and addresses the barriers (legal and otherwise) to the development of what it refers to as a trustworthy ***Identity Ecosystem***.

The critical importance of online identity management in facilitating trustworthy e-commerce and ensuring national security is now well-recognized. Several

[1] *National Strategy for Trusted Identities in Cyberspace*, at p. 1; available at http://www.dhs.gov/xlibrary/assets/ns_tic.pdf ("*National Strategy*").

ISSN 1538-3423

other governments and inter-governmental forums are already actively working to address the applicable technical and legal issues. These include Australia,[2] Canada,[3] Scotland,[4] the European Union,[5] and the Organization for Economic Cooperation and Development (OECD).[6] And now the United States has formally taken on this key issue, noting that cyberspace is a vital part of the nation's critical infrastructure, and concluding that ''a secure cyberspace is critical to the health of our economy and to the security of our Nation''.[7]

The U.S. process began in May 2009 with the National Security Telecommunications Advisory Committee's *Report to the President on Identity Management Strategy*. That Report recommended that ''the Government, working collaboratively with the private sector, the public, and interested nations, should develop a comprehensive national IdM vision and strategy that meets the security, business, and personal needs of American society and addresses the organizational, programmatic, legislative, and cultural components of IdM.''[8] Shortly thereafter, the President's *Cyberspace Policy Review* set out a 10-point Near-Term Action Plan which recommended that ''[t]he federal government – in collaboration with industry and the civil liberties and privacy communities – should build a cybersecurity-based identity management vision and strategy for the Nation that considers an array of approaches, including privacy-enhancing technologies.''[9] The draft *National Strategy* is the Administration's first step in acting on those recommendations.

The draft *National Strategy* identifies the key barriers to the development of a trustworthy Identity Ecosystem, and outlines four goals and ten objectives to address those barriers. It is all spelled out at a very high level, however, with the details (including legislative proposals) to be set out in an implementation plan to be released later in July. The goal is to finalize both documents for the President's signature by October.

The *National Strategy* makes clear that it ''does not advocate for the establishment of a national identification card.''[10] Instead, it ''seeks to establish an ecosystem of interoperable identity service providers and relying parties where individuals have the choice of different credentials or a single credential for different types of online transactions.''[11] Nonetheless, the underlying premise of the *National Strategy* is that the critical need for online identity management capabilities requires action by the federal government to make it a reality. Such actions include promoting the development of technical standards, building the required legal framework (including enacting legislation as necessary), becoming an early adopter to lead by example and to drive expectations and demand, and providing funding for private sector pilot projects. Most significantly, the document acknowledges that the legal barriers (primarily privacy and liability) are significant, and indicates a willingness to step up and try to deal with those problems, including by legislation where necessary.

Understanding the significance of the draft *National Strategy*, its impact potential on business, and the legal issues it raises, begins with an understanding of the principles of identity management, and its role in everyday online business activity.

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 in order to enter into a transaction with a third party. 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.

While there are many different approaches to identity management, it essentially involves two fundamental processes: (1) the process of identifying a person and issuing an identity credential to reflect that identity (''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''). Once an individual's identity is successfully authenticated, a third process, referred to as ''authorization,'' is used by the business relying on the authenticated identity 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.

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

[2] See, e.g., Australian National Audit Office, Attorney–General's Department Arrangements for the National Identity Security Strategy, ANAO Audit Report No.29 2009–10, April 21, 2010; available at http://www.anao.gov.au/uploads/documents/2009-2010_Audit_Report_29.pdf.

[3] Treasury Board of Canada Secretariat, Directive on Identity Management, July 1, 2009; available at http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=16577.

[4] Scottish Government, Privacy and Public Confidence in Scottish Public Services: Draft Identity Management and Privacy Principles, August 31, 2009; available at http://www.scotland.gov.uk/Publications/2009/08/PrinciplesConsultation.

[5] *See e.g.*, Commission of the European Communities, Action Plan on e-signatures and e-identification to facilitate the provision of crossborder public services in the Single Market, COM(2008) 798 final, Nov. 28, 2008; available at http://op.bna.com/pl.nsf/r?Open=dapn-8773aq; and Secure Identity Across Borders Linked (STORK-eID Consortium), Report on Legal Interoperability, Feb. 24, 2009; available at http://op.bna.com/pl.nsf/r?Open=dapn-8773ld.

[6] OECD, ''The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers'', OECD Digital Economy Papers, No. 160, June 11, 2009; available at http://www.oecd.org/dataoecd/55/48/43091476.pdf

[7] *National Strategy*, at p. 1.

[8] President's National Security Telecommunications Advisory Committee, *Report to the President on Identity Management Strategy*, May 21, 2009; available at http://www.ncs.gov/nstac/reports/2009/NSTAC%20IDTF%20Report.pdf.

[9] President's *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, (May 29, 2009), at pp. 33, 37; available at http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[10] *National Strategy*, at p. 6.

[11] *National Strategy*, at p. 6.

one or more identifying attributes (*e.g.*, name, address, height, birth date, Social Security number, employer, membership number) with a person[12] 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 contains the claimed digital identity or attributes of the person identified. As noted above, 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 smart card, ATM card, flash drive or similar device, cell phone, or computer.

When a person presents an identity credential (such as by entering a User ID on a corporate network, or presenting a driver's license at an airport), claims to be the individual identified by the credential, and seeks to exercise a right or privilege granted to such individual (e.g., to access the network or a sensitive database, to board a plane, 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, authentication is designed to answer the question ''OK, how can you prove it?'' 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.

Once a person is successfully authenticated, the relying party uses an ***authorization*** process to determine what the person is allowed to access and use. 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 (although it was never intended as such) 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 (in a closed system) 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).

The Approach of the National Strategy

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 or gaining admission to an airport boarding area.

Making this concept work in an interoperable manner in an open online environment like the Internet requires adherence by all participants (e.g., subjects, identity providers, and relying parties) to a common set of technical standards and rules of conduct, as well as appropriate risk allocation and enforcement mechanisms to ensure compliance. This set of technical interoperability standards, legal rules (including privacy and liability policies), risk models, and enforcement mechanisms is what the *National Strategy* refers to as the ***Identity Ecosystem Framework***. It is, in essence, the technical standards and the legal rules that define what each participant must do to make it all work, and how conformance with those requirements will be enforced and liability risks allocated. For legal counsel, this is the critical part. Except for some contract-based closed systems, such a framework does not currently exist. The *National Strategy* seeks to develop this framework.

The *National Strategy* follows many years of frustration in both the public and private sectors at the lack of progress in developing such a framework for truly interoperable, scalable, and cost effective federated identity management capabilities. Several systems have been built and deployed, usually within a sector-specific and limited-use context, and often with only marginal success. But the difficulties and high cost of building and deploying the technical and legal infrastructure needed for these efforts, the complexity of the processes for all participants (particularly the individuals involved), and the restricted use that could be made of the credentials, has limited their effectiveness.

The alternative envisioned by the *National Strategy* is an Identity Ecosystem Framework 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. But at the same time, it recognizes that there are numerous barriers (legal and otherwise) that must be overcome before this vision will become a reality. The barriers identified in the *National Strategy* include:

[12] Or an entity, or device, or application, etc.

- The lack of a common interoperable framework to help establish trusted identities;
- The lack of standards to promote interoperability, and insufficient resources focused on U.S. participation in national and international standards efforts;
- Legal barriers, including concerns regarding liability for providing identity-related services; concerns regarding personal privacy and the potential for unauthorized collection, aggregation, use, or release of identity information; and concerns regarding the protection of intellectual property;
- The lack of adequate available options for participants resulting from high implementation and management costs; the lack of secure, convenient, user-friendly options for user authentication and identification; the lack of diverse interoperable identity solutions; and the slow implementation pace of identity solutions generally; and
- The general lack of awareness and understanding regarding trusted digital identities.

To address these barriers, the *National Strategy* concludes that government must lead the process. Thus, it outlines a series of four general ''goals,'' committing the federal government to: (1) develop a comprehensive Identity Ecosystem Framework; (2) build and implement an interoperable identity infrastructure aligned with the Identity Ecosystem Framework; (3) take steps to enhance confidence and willingness to participate in the Identity Ecosystem; and (4) take steps to ensure the long-term success of the Identity Ecosystem

To help jump-start the process, the *National Strategy*'s four goals are supported by ten ''objectives.'' When viewed together, these objectives essentially propose that the federal government will take the lead in driving the process for the development of required standards; enact required legislation (particularly privacy and liability legislation) to address the legal barriers; incentivize private sector development and take a lead role in implementation by being an early adopter (to leverage its buying power and to help drive expectations and demand), by funding private sector pilot programs, and otherwise incentivizing interoperability of private sector solutions; and provide assistance in ensuring awareness and education.

Building the Legal Framework

A legal framework is required for federated identity systems of the type envisioned by the *National Strategy* to function effectively. Such a legal framework should:

- clearly define the rights, responsibilities, and performance obligations of all of the participant roles (e.g., subjects, identity providers, and relying parties) so that the process works properly, effectively, and reliably to establish the required level of trust;
- operate in compliance with all existing laws including those governing the privacy and security of personal information, and requirements for the authentication of individuals in online transactions;
- fairly allocate among the participant roles the legal risks involved;
- 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); and
- provide realistic enforcement mechanisms and remedies in the event that a participant fails to act in the required manner.

Although the need for such a legal framework is generally acknowledged, developing it is uncharted territory. There are numerous legal issues and legal barriers that must be addressed, and one group, the American Bar Association's Federated Identity Management Legal Task Force,[13] has recently undertaken a project to identify and analyze those issues. 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 federated 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 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 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 Ecosystem Legal 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 healthcare 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 the Identity Ecosystem Framework ''must provide strong privacy and security protections to individuals in addition to creating clear rules and guidelines concerning the circumstances under which a service provider or relying party may share information and the kinds of information that they may share.''[14] Thus, the *National Strategy* contemplates new privacy requirements, based on the Fair Information Practice Principles,[15] which would presumably be enacted by new legislation.

In addition to legislation, the *National Strategy* seeks to address the privacy issue by shifting from the current

[13] Federated Identity Management Legal Task Force, Cyberspace Committee, ABA Section of Business Law; information available at http://www.abanet.org/dch/committee.cfm?com=CL320041.

[14] *National Strategy* at p. 23.

[15] *See National Strategy*, Appendix C, at p. 36.

enterprise managed approach to identity systems (typically for a singular purpose with a single relying party) to what it refers to as user centric systems. Under a user centric approach, users 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.[16]

Resolving these privacy issues by legislation or regulation 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 concern of all participants in any Identity Ecosystem is determining who will bear the risks associated with failures of performance, faulty identification or authentication, failure of technology, and other problems that might lead to unauthorized access or circumvention of access controls through identity fraud or mistake. These concerns about liability include questions such as:

- 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 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 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.[17] Yet at the end of the day, the legal risks remain ill-defined and 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. And it understands that the information it provides will be relied upon by parties to a business transaction. It is this aspect of reliance that is critical. Both the identity provider that issues an identity credential, 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 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, 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 existing legal uncertainties with respect to this issue are a major barrier to the implementation of a trustworthy identity ecosystem. 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 *National Strategy* recognizes that concerns around liability represent a key barrier to private sector adoption of interoperable identity management solutions, and takes the view that legislation many be necessary to address those concerns. In fact, it specifically notes that:

> Key elements of the Identity Ecosystem Framework are defining the rights and responsibilities of the various participants in the Identity Ecosystem and establishing an enforcement mechanism, if participants do not carry out these responsibilities. To define these responsibilities, the Federal Government must address liability issues within the Identity Ecosystem (e.g., should there be liability caps or floors on identity providers if credentials are fraudulently used?). These liability concerns have historically prevented organizations from providing and using identity and attribute provider services. The Federal Government needs to establish new or amend existing policies and laws to address these liability concerns and to establish the enforcement mechanisms that provide accountability.[18]

Other than to suggest that some form of legislation is needed, however, the *National Strategy* does not provide any answers to the liability dilemma.

Path Forward

The *National Strategy* expresses a need for the federal government to push the agenda, and the intent to do so. But this is all at a very general level. The devil is in the details yet to come. That will presumably take a more concrete form in the implementation plan to be released shortly. And then the debate will likely begin in earnest.

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

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

[18] *National Strategy*, at p. 22.