INTERNATIONAL TRADE ADMINISTRATION

IDENTITY MANAGEMENT AND INTERNATIONAL BUSINESS COMPETITIVENESS: A ROUNDTABLE DISCUSSION

The following is a summary of the Identity Management Roundtable, compiled by James Lewis, Senior Fellow and Director for Technology and Public Policy Programs at the Center for Strategic and International Studies. The Office of Technology and Electronic Commerce expresses its appreciation to Mr. Lewis for serving as Rapporteur and preparing this report.

Rapporteur's Summary, October 10, 2007

On September 18, the Department of Commerce's International Trade Administration (ITA) held a roundtable with twenty-five panelists from the private and public sectors on identity management and international business competitiveness. The purpose of the roundtable was to gather a group of experts from civil society, industry, and government to discuss the current identity management policy landscape, policy trends, and how to best address the development of identity management policies. The roundtable discussion was divided among four topics: 1) the current identity management landscape, 2) how identity management practices affect competitiveness and potential barriers to international data flows, 3) the ability to use e-commerce to expand international trade, and 4) how government and industry could work together to resolve issues. Each topic was introduced by two of the participants, who provided a brief overview of the issues. These introductory remarks were followed by group discussion.

Identity management can refer to how a company manages personally identifiable information (PII) for employees, partners, and customers. PII has become a major concern for companies as they face an array of new rules and requirements. Internal and external processes for transactions involving PII are merging within companies, in order to take advantage of new technologies and to gain efficiencies, creating new kinds of identity management problems.

During the roundtable discussion, many participants expressed the opinion that there are common views in a number of broad areas on how identity management could be improved to enable e-commerce, but also revealed multiple, and sometimes conflicting, definitions and approaches to specific issues. Two particular issues recurred throughout the discussion. The first was how to define the role of government in advancing identity management in ways that promote international e-commerce (and what role ITA could play in this effort). The second was a discussion of the nature and elements of an effective and acceptable identity management system and what role, if any, would be appropriate for government (including the Commerce Department) to play in developing this system.

The view of most participants was that government can facilitate and accelerate the development of common approaches to the treatment of PII, and that these government efforts should preserve flexibility in emerging rules and policies. As one participant put it, government should not play the game, but it should provide the playing field (e.g. ensure the rules allow companies to compete effectively and fairly). As part of this "provide the field" approach, some participants observed that the prescriptive approach to policy that was taken in many previous governmental

efforts to improve online identity and authentication had doomed these efforts. Avoiding a prescriptive approach will be essential as technologies and business models for identity management continue to emerge and evolve.

Flexible approaches to policy and legislation are also essential if there are to be consistent rules for managing PII among different countries. Conflicting or contradictory rules for identity management will be a serious obstacle to the new, globally integrated forms of commerce that have begun to emerge in the last decade. Agreement among countries will be difficult, however, unless it is initially limited to general principles or guidelines for national policies and regulation. The goal is to avoid a *fait accompli* that accidentally or intentionally locks out new technologies or ways of doing business.

The attributes of a good identity management system that were identified by participants during the discussion seemed to flow from a widely shared view that whatever form identity management ultimately takes, it will need to accommodate a diverse environment for many years to come. As explained by one participant, interoperability among identity management systems is necessary because there will be multiple identity management solutions that must be able to work together. The need for interoperability applies not only to technology, but also to policies. Participants expanded on that theme by noting that the ability to accommodate diversity (in both business practices and technologies) will be a critical attribute for identity management systems and a crucial component of a "good" system. Diversity in technologies, uses, and rules are a given, and policies that do not recognize this will become either irrelevant or obstacles. Accommodating this diversity will require interoperability and openness.

A number of participants expressed the opinion that "openness" will be necessary for identity management systems and to accommodate diversity in processes and technology. Openness is a charged term and its definition is still imprecise, but many participants agreed that openness is linked to interoperability, and to the extent to which openness means that systems or technologies that provide the same outcomes (for privacy, security, and identification) should be treated the same way, it is an important element of interoperability.

Participants also expressed the opinion that identity management (and accompanying policies) should be driven by successful business models, since the experience of the past has shown it is quite possible to build identity management systems that protect privacy, meet legal requirements, and are secure, yet at the same time have little or no appeal or benefit for business and consumers.

Throughout the roundtable discussion, participants referred to the payment card industry (PCI) as a useful precedent for how to manage PII. Several participants recommended that policymakers and industry look at the PCI rules as one approach to an effective system of data security. The PCI model points to the need for a business case for identity management. In the PCI example, the business case was created when legislation shifted liability for credit card losses due to fraud from consumers to companies. By eliminating consumer liability, the government created a powerful incentive for banks to develop effective security and anti-fraud policies and technologies.

Another constant theme in the discussion was the repeated caveat that government should not create policies that dictate technology development. In itself, as advice to avoid prescriptive policies, this is an important point. However, the issues are more complex, and experience (such as the effect of legislation on PCI) suggests that policy must be more than the handmaiden of

technology since the absence of adequate policies of identity management is an impediment to progress. A more nuanced approach to government intervention—one that sets goals and standards but avoids requiring specific technologies or processes—is most likely to expand e-commerce. Further exchange of ideas on whether there is a "policy gap" and how this impedes or distorts identity management could help set the stage for the next generation of e-commerce.

Session I – Identity Management Practices

Participants started this session by noting that the current environment for identity management is shaped by diversity. Making the pieces of this diverse environment—commercial, legal, and technical—fit together will be a major challenge. This challenge will only grow as we enter a new phase in the use of digital network technologies. Whether we call it cloud computing or Web 2.0, consumers will use the Internet in new ways that use web-based applications and remote storage of personal data. The advent and growth of Web 2.0 has resulted in more opportunities for Internet users to make their personal information available to the public, through online services like social networking websites. Because technology has advanced to the point of untethering applications from geography, consumers will connect to a Web service without knowing its physical location. How these new Web services are deployed and used will be determined in part by how well the IT community succeeds in improving identity management. Many participants noted that fragmented and opaque identity management practices increase risk and will limit the growth of e-commerce.

A number of participants pointed out during the first session that one benefit of a good identity management system is that it would reduce the need for providing and storing PII. This would minimize the amount of PII required for a transaction. Online authentication in many instances simply replicates the paper processes that predated the Internet. We have used new technologies to continue old modes of identification. To engage in a transaction, a consumer is asked to fill out a form providing name, address, and other data; this data is then retained by the receiving party, when all that is really required is the ability to confirm identity in a trustworthy fashion. A good identity management system would take a "surgical approach" to the use of PII and enable transactions without creating vast repositories of data. This could reduce both the amount of PII used in an individual transaction and the flow of PII between companies and across borders.

Several participants expressed concern over these paper-based practices to authenticate identity because these practices have made it cheap and easy to dip into the "information cloud" to collect PII from various sources, which can then be assembled into a comprehensive set of PII for an individual. Improving identity management in this new Web 2.0 environment depends to some degree on progress in improving online authentication of identity. As one participant noted, identity started with the physical individual, but has now developed into a larger "cloud" of credentials and aliases that individuals use to identify themselves in the online environment. Authentication is the process by which a company or individual assesses the degree of trustworthiness or risk associated with a credential, and effective authentication could allow companies to decide when a credential can take the place of collecting or storing PII.

We usually look at identity management from the institutional perspective, but it is also important to look at how individuals manage the use of their own identity information as a means of safeguarding privacy and limiting uses of their PII; these individual efforts shape and limit online transactions. The lack of ubiquitous systems for individuals to authenticate their identity on the Internet is an obstacle for e-commerce and makes identity management more complex.

Weak identity management creates unnecessary risks to privacy. Weak authentication increases risk in online transactions for consumers and companies. In order to authenticate themselves in a transaction, individuals are asked to provide PII over and over again—name, address, and other data—a trail of "digital breadcrumbs" as they traverse the Internet. The lack of alternatives for authenticating individuals means that companies collect PII and hold it, creating risks for both themselves and for consumers. Better authentication systems would limit the "digital breadcrumbs" that lead back to an individual's PII and eliminate the associated risks.

Discussion of the linkage between data security and identity management during this session was somewhat ambiguous. While there was acknowledgement that the linkage between data security and identity management is important, some participants stated that it is also important to avoid considering identity management as solely a security issue. There are technologies that could reduce risk and improve identity management, but these technologies are not widely deployed. More importantly, the technologies used for identity management are often not interoperable, nor are there agreed processes on how they will be used or how the information they require will be used or stored. Getting all the parts of identity management to work together – the commercial requirements, technologies, policies and rules—will be a major challenge for both the public and private sectors.

There are models and precedents, however, for fitting the pieces together. The Internet is a successful distributed system, where diverse and numerous sets of companies, organizations, and individuals are involved in its operation and development. The Internet model, with its use of common standards that accommodate diverse technologies and its minimalist (so far) approach to governance is a useful guide for better identity management.

The goal for policy cannot be the pursuit of a single overarching system for authentication and identity management. Models that accommodate diversity are more likely to allow progress. One model for these distributed authentication systems is federation. Federation is an approach to governance that allows multiple, independent, and heterogeneous systems to work together. Federations work best when a basic document sets out how the entities will cooperate, defines their responsibilities and the responsibilities of the federation, and creates mechanisms for dispute resolution and administration (this set of activities is sometime called "governance"). A federated approach to authentication means developing a common set of rules that will allow identities issued by different processes and places to be recognized and treated equally. These rules will need to establish baselines for the various processes involved in identity management (such as enrollment or revocation). The goal for policy is to ensure that while the procedures used by different authentication systems differ, the outcomes will be the same.

At the conclusion of this session, many participants expressed the view that effective identity management systems will use a federated approach based on open standards to ensure interoperability. Federation among different identity systems is the governance system that best accommodates diversity. Federation involves creating a framework of agreements under which different identity systems can interoperate. However, federations rarely appear spontaneously, and with the identity management landscape in a state of flux, industry and government lack incentives and processes for adopting a federated approach. As part of an effort to expand federated identity, the sense of many participants was that ITA could play a useful role in helping to get international institutions to develop the framework or common policies needed for federation. This framework could help to provide the basis for "making the pieces fit together" on the international level.

Session II - Expanding Global e-Commerce

Two crucial points emerged in the discussion of how identity management can contribute to the expansion of global e-commerce. The first is that internal and external transaction processes are merging in many companies. This merging of processes is reshaping and strengthening the business case for better identity management as it changes how companies and their customers use and save information.

The second point is that some of the challenges presented by identity management are not entirely new, particularly the issue of how to meet international concerns over privacy protections for citizens of countries with different legal environments. Effective identity management systems will need to work across national boundaries, but as governments create regulations and policies for protecting personal data as an identity management element, interoperability and consistency of regulation for identity management will be more difficult.

The core of the problem lies at the intersection of company practices and national laws. Countries are introducing or extending regulations for identity management (addressing both privacy and security) in which identity management becomes a subset of policies that govern the use of PII. This approach, absent change, will force companies to face different and potentially conflicting regulations in different countries, with the unintended effect of slowing the development and implementation of new services and business processes.

This emerging policy landscape for identity management points to a critical role for government - promoting "policy interoperability." A focus on technological solutions alone will not build interoperability. Policy interoperability needs common understandings or agreements among governments on identity management policies, but it will also need some kind of accountability and enforcement mechanism, voluntary or otherwise, that binds companies to observe guidelines, such as how much PII is required for a transaction and how or if it is stored. How the questions of enforcement and accountability are answered will determine if consumers view identity management efforts as effective and trustworthy.

Many participants remarked that the lack of policy interoperability will be a serious obstacle to e-commerce, as globally connected businesses are confronted with different and varying requirements imposed by different governments. They further noted the development of global standards (or less ambitiously, consistent regional standards) for identity management will help avoid the problem of companies being required to meet multiple and conflicting sets of requirements for authentication, privacy, or other elements of identity management. If agreement on principles governing identity management among governments can be reached, it will help avoid a situation where there are multiple rules governing identity management. A fragmented approach to PII and uncoordinated rulemaking by governments will create problems for commerce, competitiveness, and innovation.

Many participants thought that it would be difficult to reach agreement among different governments on principles or standards if these principles were too detailed or specific. They noted that global standards may require generalized rules—generalized in the sense that they avoid prescribing specific technologies or approaches for identity management, yet provide consistent policies that work across different legal jurisdictions, which should ideally result in guaranteed privacy while allowing identity management systems to work together across borders. In this regard, the issues raised by identity management for global e-commerce are similar to the data flow problems of a decade ago, and the resolution of the data flow issue

through the Safe Harbor Agreement may provide useful precedents upon which we can draw.

Session III - Improving the Identity Policy Landscape

Several participants observed that the appearance and growth of online services is causing the policy landscape for PII and identity management to shift rapidly. What worked in the late 1990s may no longer be appropriate for the new technologies and the new e-commerce environment. Various participants also stated that with few exceptions, there are neither shared best practices nor common technologies to manage and secure PII, even though the collection of PII is a standard element of e-commerce.

A number of panelists observed the need for policy change that is independent of changes in consumer attitudes toward privacy because of the effect of new web services. Some participants suggested that social websites like Facebook or YouTube suggest that consumer attitudes toward the treatment of PII have changed, and that a younger generation of consumers who are accustomed to the web have a different set of concerns (or degree of concern) and different levels of understanding when it comes to protecting PII. Other participants argued that these new behaviors do not, however, translate into an assertion that a new generation of consumers is less worried about privacy, and the notion that consumer interest in protecting PII has decreased should be approached with caution. While this new generation of consumers may be willing to release information relating to their social life, it is not clear if this carries over to financial matters.

One participant told the story of a recent Washington Post article that explained the plight of a young job applicant whose efforts to find work were damaged by false information on the Web; several participants speculated that occurrences like this might produce a retrenchment in the previous wide-open attitudes toward some personal information. They believe there is a growing concern among consumers over the reputational effects of social websites, and that this concern may indicate that deeper attitudes and concerns regarding PII have not changed as much as we may think.

They also noted that after more than a decade of experience with the Web, we are seeing more sophisticated users who will, in the absence of better identity management, use a variety of techniques, including pseudonymity, to protect or conceal PII. With evolving online services, privacy preferences are changing, but the protection of PII remains important for consumers, and continued data breaches by online merchants may lead consumers to opt out of certain categories of transactions.

A related set of issues discussed by the participants involved determining what information is really needed for a transaction. The amount of information may depend on the degree of risk – a high-risk transaction could require more PII than a low-risk transaction. Alternatively, several participants reiterated that the requirements of a high-risk transaction could be met with improved online authentication, by reducing the amount of PII (when it is collected in order to authenticate identity) needed for a transaction. This could take the form of "partial identities," where only the PII necessary for a transaction would be transferred, or the creation of some system that avoids the need to transfer data entirely (thus circumventing the requirements of potentially onerous PII regulations without putting privacy at risk).

Creating robust authentication alternatives for online transactions will require the development of both technical specifications and legislation. Some technical specifications for identity

assurance have already been developed by the International Telecommunication Union (ITU) and by the National Institute of Standards and Technology (NIST). Governments can use these standards as a starting point basis for a discussion of the policies needed for trust and assurance.

Many participants believed that progress in policy will be driven by business needs. This progress will require insight into three issues: a better understanding of what privacy means and what privacy protection entails in the new digital environment; a clearer notion of what a good identity management system would look like (in terms of safeguards for consumers and assurance levels for business); and a business case, perhaps incentivized by governmental mandates to protect PII, for moving ahead. In each of these three areas, there was some agreement on how to move ahead, but this consensus exists at only a high level. A discussion that focused on specifics would likely find, at least initially, wide areas of divergence.

Session IV - The Role of Government and Industry

Discussion of the role of government and industry highlighted the interrelationship between public and private sectors in developing effective identity management policies. The discussion also pointed to an underlying problem confronting governments; addressing PII and identity management in the policy arena is a slow process, but it is easy and quick for businesses to change their business practices. This ability of businesses to change the underlying elements of an identity management system (the particular attributes used) dictates what kinds of policies will work best if our goal is to expand e-commerce – those that are flexible, avoid specificity in means, and yet set clear goals for companies to meet.

It would be very difficult to create a single framework to address the multitude of privacy needs for consumers and industry. Instilling trust is an important step, but sometimes government does things that decrease trust, like misusing technologies for surveillance purposes. Most participants were of the view that it would be best to use existing bodies (such as the OECD and APEC) to develop these general recommendations and principles for identity management.

A few participants suggested that we need to question the assumption that online transactions are inherently more risky. Most data suggests that fraud and identity theft are more likely to happen in a bricks-and-mortar setting than in virtual transactions. Some even argued that the distinction between offline and online is artificial. Several participants suggested that educating the public about the nature and level of online risk would be helpful, and that this could require developing adequate indicators to show that e-commerce is safe. Comprehensive statistics on identity theft, online sales, and security breaches could help create benchmarks to measure identity management and privacy for online transactions and provide a guide for policymaking. Government can help to educate and "market" information so that the message gets through to consumers on how to protect PII.

Some participants felt that an important function for government would be to raise awareness among officials and the public of the challenges of identity management. Consumers and regulators only have access to "imperfect information" with regard to technology and the web. We need to advance the 'state-of-the-art' in knowledge for consumers and regulators. We need to remember, however, that raising awareness by itself is a poor substitute for substantive measures. After more than a decade of discussion on privacy, digital signatures, e-commerce, and PKI, raising awareness is no longer enough to improve identity management and it should not be the central focus for policy makers.

Education is a useful supporting step for expanding e-commerce internationally, but it is at times a stalking horse for those who prefer inaction and it should not be the central focus for policy. There are a number of things that governments can do, however, to advance identity management. First, government can act as a vehicle to resolve some of the issues relating to identity management by being a facilitator and providing the means of coordinating with other governments. At a minimum, the coordinating role can provide a defense against bad foreign identity management policies (multiple national rules will create problems for international commerce), but ideally it would involve actively engaging foreign governments, using existing relationships and organizations, to develop identity management policies that further enable international e-commerce. Government can also help by being an early adopter through procurements and regulations (although this is not a role for ITA).

Next Steps

The Roundtable began with the group identifying two central issues: what would good identity management entail and what should be the role of government in helping to create this. In discussion of the two issues, the recurrent underlying theme was that identity management will be a key element for international e-commerce. Weak identity management will lead businesses and consumers in one direction—toward activities that minimize risk but also minimize the chance for growth. Better identity management will make it easier to benefit from new web technologies and to manage the many concerns surrounding the use of personally identifiable information.

The roundtable discussion made it clear that making identity management work to expand international e-commerce is not a technology problem. There are many good technologies, but they operate in a policy vacuum or "policy gap." The technology may be trustworthy, but the environment it operates in is not. There is a role for government in remedying this situation in encouraging the development of governance systems.

In discussing the role of government, participants expressed a number of caveats based on previous experience with authentication and e-commerce. The gist of these admonitions was the need to avoid prescription and to ensure compatibility among differing national rules. A related discussion revolved around whether policy should lead technology or vice-versa. Since technology has led policy for more than a decade—with very little to show for it—this relic of the dot.com era would not seem to be a good idea. Nevertheless, the point about avoiding a "digital signature" approach, where specific technologies and business models were prescribed by law (to the detriment of all), remains valid.

However, avoiding a prescriptive approach to policy is not a recommendation for governmental inaction. Absent government intervention, progress in identity management will likely be slow and circuitous. Government action can accelerate consensus on identity management and ensure policy interoperability. Participants expressed the view that this action could best take place in existing multilateral bodies (rather than creating a new group or process), and the United States should consider "safe harbor' as a useful precedent.

The precedent of the Safe Harbor Framework between the United States and the EU remains one of the best guides for how to move ahead in developing a common international approach to identity management. That agreement allows U.S. companies to comply with the data protection of the EU by certifying that they meet the privacy principles of the Safe Harbor agreement between the United States and the EU. The agreement averted a situation where U.S. companies

would have faced serious obstacles to participating in European e-commerce.

International engagement on identity management could become a critical mission for ITA. International engagement between U.S. companies and the U.S. government with their foreign counterparts could foster interoperability and consistency of identity management systems and policies. The web is changing and e-commerce will change with it, in ways that will make existing rules inadequate or into obstructions. The goal for policy is to protect PII while preserving the necessary flexibility as technology and commerce continue to evolve.