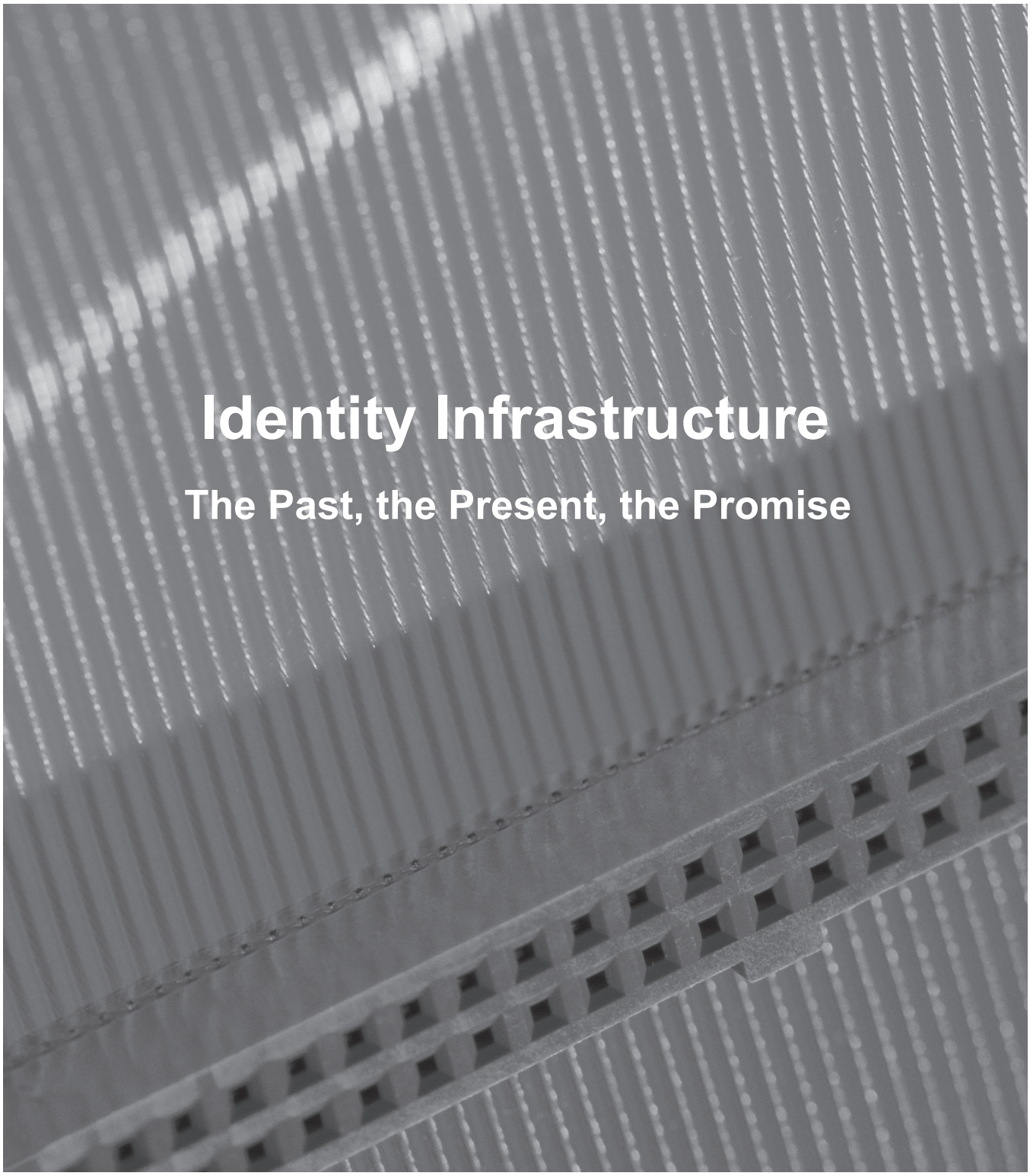

Identity Infrastructure

The Past, the Present, the Promise

Prepared by the Technology of Identity Work Group

National Electronic Commerce Coordinating Council (eC3)

Presented at the 2006 eC3 Annual Conference, held December 4-6, 2006, in Sacramento, California

eC3
449 Lewis Hargett Circle, Suite 290
Lexington, KY 40503
859-276-1147
www.ec3.org

Made in the United States of America

A consortium of national organizations and public & private sector leaders identifying best practices for strategic change within government

NASACT - National Association of State Auditors, Comptrollers and Treasurers
NASS - National Association of Secretaries of State
AGA – Association of Government Accountants
ALGA - Association of Local Government Auditors
ITAA - Information Technology Association of America
NACHA - National Automated Clearing House Association
NACo - National Association of Counties
NAGARA - National Association of Government Archive and Records Administrators
NAST - National Association of State Treasurers
NIGP - National Institute of Governmental Purchasing
PTI – Public Technology Institute

Introduction

The National Electronic Commerce Coordinating Council (eC3) issued its first whitepaper[1] addressing the topic of Identity Infrastructure in 2003. The topic was a "hot-button issue" that year and the concept in its infancy. There has been a lot of progress since 2003 on identity issues such as governance, business models and technology. The EC3 commissioned a work group to take a new look at past work and project another three to five years into the future of identity infrastructure.

The workgroup was composed of thought leaders from government and industry - many of whom have long experience in policy and practice related to identity management and identity infrastructure. This paper is intended to provide to public sector, industry, and standards setting groups the latest information and projections on identity infrastructure. The intent is to inform decision makers who will develop, deploy and use identity infrastructure. This will be done in the context of issues of digital rights, digital privacy, digital identity and responsibility for all e-life participants.

Most people who work or write on identity-related issues believe that action is desperately needed to realize the full potential of identity management. Even those most concerned about potential downsides such as compromise of privacy or loss of personal information seem to agree that we need to improve identity functions and handling of personal information. The authors are cautiously optimistic that identity management can improve, but that it will require effort and commitment on the part of practitioners as well as cultural changes. Current expenditures for performing identity functions coupled with losses due to performing them badly are many times the cost of implementing and maintaining improved systems and practices. It will be difficult to redirect resources from where they currently flow to an improved identity environment, but the consequences of maintaining the status quo are far too severe to do otherwise.

Evolution and Change: A Brief History of Identity

Early computer users in order to use the equipment had to enter the room or building housing the computer hardware. Controlling access to the room significantly limited access to the computer. A series of developments of networks further and further distanced users from the equipment until development of Internet created the means for users to access computers around the globe. Early on computers were used to process information. Ask the right questions in the right way, feed it the right data and it will work away to sort, collate and come up with an answer.

During this early progress in networking computers there was a parallel development of the volume and value of information stored in the machines and value of transactions that could be completed across the networks. The more valuable the assets the more likely they are to attract mischief-makers and criminals and the more important it becomes to control access to these resources. Early access

[1] Identity Infrastructure, National Electronic Commerce Coordinating Council, Manage Identity Work Group – Infrastructure Sub Work Group, November 2003, www.ec3.org/Pubs.

control involved a simple account number more for tracking and billing than security and was performed on a single computer or built into individual applications. As the value of the resources and thus the risk involved with access grew it became ever more important to control who could get into the system and what users could do once inside. Controlling access often has been accomplished by identifying a user and providing methods of authenticating that user to the system when access is needed. Systems employing usernames, PINs and passwords soon followed and quickly grew in complexity and security. Further advancements included the use of devices and the checking of biometrics to increase the security of the access control mechanism. These access control and related functions have come to be known as identity management (IDM).

The various functions comprising IDM such as identity verification, provisioning, maintenance and operation of the system become more expensive and more difficult to perform as the requirement for greater security grows. Similar processes, systems, and costs are involved to reach a particular level of security whether performed for a single application or for many. When built into individual applications the same functions are repeated multiple times requiring users to register multiple times, remember multiple sets of information and/or use multiple access processes. The cost and complexity of performing IDM grew to a point that eventually catalyzed efforts to rein in total costs while further improving security.

As the practice of identity management grew it has been abstracted from individual applications often becoming a stand alone service providing functions to numerous applications or an entire enterprise. The skills of invaders continue to grow, with online communities providing training, tools, techniques and even markets for criminals, driving ever more complicated and expensive IDM requirements. The increasing cost and skill involved in providing IDM functions is resulting in enterprise IDM and the creation of identity federation or IDM across organizational boundaries. Once identity functions have been abstracted from individual applications and performed across an organization it is just one more step, albeit a substantial one, to share those functions among organizations. The components of identity functions, the policies, services, hardware and software, can be distributed across wide geographic and virtual divides. Bridging these divides requires an identity infrastructure. This developing identity infrastructure is the subject of this paper.

What is Identity Infrastructure

An Identity Infrastructure is a collection of components including policy, processes and technology that facilitates identity functions such as identity proofing, verification, provisioning and authentication in support of other interactions or transactions. Think of the Interstate Highway system or the electrical infrastructure. Each homeowner and business could buy a generator and supply its own electricity, but if each also had to design and develop the lights and circuits and electrically driven devices or choose from those using various voltages, wattages or plug sizes then the value and usefulness would be significantly less. The identity infrastructure is bringing together organizations that verify users' identity information and issue credentials (power companies?) with organizations needing these services and their users. Sometimes these are the same organization but often not. These services may well be outsourced to operations specializing in performing the various processes. It took decades to standardize electrical infrastructure components, develop business models to support distribution and build the distribution grid.

Why is it important

Building an electrical infrastructure gave people a tool with which to improve their lives. Innovators developed tools and machines that would use electricity as their source of power. The electrical machines alleviated a lot of physical drudgery. Pumps moved water doing away with the back breaking toil of carrying it. Washing machines eased the work of cleaning clothes. Power tools removed a great deal of physical labor from construction. Electricity provided better, safer lighting for our streets making us safer. While easing the physical burdens of labor the electrical infrastructure helped to catalyze a reengineering of society and changed us in myriad ways.

The developing identity infrastructure will have far-reaching and in many cases similar consequences. It will change ways we interact, make us safer and catalyze reengineering of business and government. It will reduce losses to identity related crimes, reduce costs for identity management and security and slow funds flowing to terrorist and criminal organizations. Development of the identity infrastructure will help to allay user fears and quicken adoption of online services.

What happens if we ignore the problem

Given all of the efforts underway it is not feasible to ignore identity related problems, but what would happen if a choice was made to slow down work currently underway or to otherwise put off development of an identity infrastructure? Evidence indicates that identity related crimes are still increasing although the rate at which they are increasing may have slowed. The actual rate of such crimes is difficult to determine due in part to the fact that identity crimes are not discovered for up to 18 months after they occur. It is certain that organizations will continue to implement technology solutions and to waste more resources as those solutions are implemented at less than optimal levels. With less focus on infrastructure and its benefits there would likely be more integration and reengineering required at some point in the future.

As more people become victims and trust in the system further erodes there will occur a crisis of trust. People will refuse to trust electronic systems, which at this point means most of our business and government in some form or other. On Black Monday, 1929 (and 1987 for that matter) nothing was drastically different for the financial markets, except that people lost trust and panicked. The stock market drops were the result of people losing their trust in the system. It is foreseeable that if today's losses to identity crimes continue, people will lose their trust in the electronic systems of today. Some of this is already being experienced and is evidenced in slower than projected adoption rates of electronic services. While these slower adoption rates increase costs and reduce anticipated savings, they are nothing as compared to the disruption and cost of a panic. The current reliance upon electronic processes for business and government coupled with a widespread panic would entail huge disruptions to society and commerce. No one knows for certain where the threshold of panic is, but it does seem fairly certain that there is one. That point will be reached sooner rather than later if the problems are not addressed.

The State of Identity 2006

The three years since 2003 have seen continued rapid growth in losses resulting from badly performed identity functions that create easy targets for criminals. Costs of performing these functions also continue to rise. Spending on and adoption of improved identity functionality lags well behind needed levels to repel rapidly evolving threats. (See box at right on Data Breaches.) There has been a lot of work performed and investment made as more organizations become involved in addressing the related problems but more is needed. A great deal of media attention has been focused on the topic and the level of public understanding of the need for improved identity functions has risen but much more can and should be done.

The toll for 2006:

- An estimated $50 to $60 billion in direct losses, twice that when remediation and recovery costs are included
- 10,000,000 U.S. Citizens discovered they were victims of identity related crimes
- Online criminal communities, such as Shadowcrew, provide online "malls" for identity criminals
- Dozens of system breaches requiring public notification, lost equipment containing U.S. citizen and resident personal information, data tapes "falling off trucks"
- Anecdotes of terrorists using identity related crimes to finance operations
- IT Pros Say They Can't Stop Data Breaches (please see box at right)

Progress

- Federations are operating to the benefit of participants
- EAP working to develop federation interoperation
- Real ID is passed
- Lots of activity by a widening array of organizations

IT Pros Say They Can't Stop Data Breaches

By Deborah Rothberg
August 30, 2006

Updated: Nearly two-thirds of respondents in a new study say they're ineffective in preventing data breaches.

In the wake of widely publicized security compromises at AOL and AT&T, a study released Aug. 28 by the Elk Rapids, Mich.-based privacy management research company Ponemon Institute finds that only 37 percent of IT professionals believe their company is effective at detecting data breaches.

Citing a lack of resources and high product costs as barriers to preventing data leakage, respondents were uncertain about their company's ability to discover breaches of confidential information. Only 43 percent believed that their company would detect a large breach (involving more than 10,000 customer records) more than 80 percent of the time. 17 percent of respondents felt their company would correctly detect a small data breach (involving less than 100 customer records) more than 80 percent of the time.

"We've gotten pretty good at protecting from spam and viruses. But, when you rob a bank, you go for the money, and that's the data. Companies are beginning to shift their priorities away from the perimeter and onto the information content," said Gordon Rapkin, president and CEO of Protegrity, a Stamford, Conn.-based provider of enterprise security management solutions. (From eweek.com; http://www.eweek.com/article2/0,1759,2010325,00.asp)

During the three years since publishing the previous eC3 paper on identity infrastructure there have been several efforts undertaken. [2] The E-Authentication Initiative (later the E-Authentication

[2] Refer to the variety of presentations available on the eC3 web page at: http://www.ec3.org/Pubs/PubsConfPresentations.html

Federation) has been developed and incorporated into the Federal Enterprise Architecture. The E-Authentication Partnership has been created and is operating. The Federation for Identity Cross-Credentialing Systems, FiXS, has been developed to facilitate interoperability of physical access credentials across government and contractor facilities. Secure Access for Everyone (later Signatures and Authentication for Everyone) SAFE has been developed and is providing service for pharmaceutical companies and government as is InCommon, a Shibboleth-based federation for educational institutions.

The year 2005 saw the U.S. Congress pass the Real ID Act which is estimated by some to cost $11 billion to implement. The Federal Government has undertaken multiple efforts to address identity function needs. Other levels of government and non-government sectors have spent untold billions of dollars to meet identity management needs. All of these organizations have recognized the necessity of performing these functions better and are dedicating scarce resources to attempt to meet their needs.

We created these problems ourselves. Prior to 9-11-2001 any attempts by government personnel to undertake development of robust enterprise level or cross-boundary identity management systems were mostly met with disdain or derision. Often such efforts would have been looked upon as inappropriate for involvement by government. It is this unwillingness to address the need for identity infrastructure that creates the gaps through which criminals and terrorists attack resulting in the current situation. Government has been negligent by not providing for the identity needs of our society.

The Challenge

- Issues are misunderstood
- Change will be required throughout U.S. society
- Attitudes vary dramatically
- Benefits are disputed
- Public or customer resistance is feared
- Problem cannot be solved only addressed
- U.S. has desperately underestimated the problem and under spent to meet the challenge for years
- Criminal attacks will continue to evolve faster than prevention

While some improvements are being made as a whole identity functions in this country are falling behind "state of the art" criminal attacks. It is likely that even moderately skilled or ambitious amateur criminals can effectively compromise most systems. Many industry verticals are addressing their own versions of identity related crimes and associated security and access issues. Here is discussed the financial sector, but a similar case could be developed for several other industries such as health or retail for example. The U.S. Federal Government's Federal Financial Institutions Examination Council(FFIEC) Agencies, including the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision, issued a statement as follows: "The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties."[3] There are a number of possible approaches offered to improve upon single factor authentication. The FFIEC letter includes the recommendation that "insured institutions should use multifactor authentication, layered security,[4] or other appropriate controls[5]" and allows for a variety of relatively modest security industry standard solutions. There were/are many in the financial industry that question potential benefits and express substantial concerns over customer resistance and implementation costs of the recommendation.

It is important to note that some financial institutions have undertaken to improve safety

Manner of Perpetration

Understanding exactly how identity theft is perpetrated can help regulators, institutions, and consumers identify ways to stop this form of fraud. All identity theft begins with a security compromise of confidential personal data, but linking the security compromise of personal data with the identity theft perpetrator and/or the perpetrator's means of access is difficult and often impossible. These crimes are often unreported and not prosecuted, and they often cross geographic and legal jurisdictions. Victims are unlikely to know that third parties or insiders have stolen their confidential information, or unlikely to be aware that computer spyware, a virus, a hacker, or even phishing is the direct cause of their problem.[6] The more technologically challenging the case, the less likely it is that the victim will understand the means of access.

Two recent studies explore how identity theft is perpetrated. Data from one study do not support the conclusion that "most thieves still obtain personal information through traditional rather than electronic means." [7] As noted above, victims of sophisticated electronic fraud are unlikely to understand how the fraud was perpetrated, so estimates of means of access to confidential information must be interpreted cautiously.

Another study sheds light on a narrow range of identity theft: cases that resulted in arrest or conviction. Although the sample underrepresents the more sophisticated types of electronic fraud as well as crimes that cross legal jurisdictions and all those that are never prosecuted, even for this limited sample it is noteworthy how often the alleged or actual perpetrators acted with others and used the identities of one or more businesses or created bogus businesses to effectuate the fraud.[8]

This article and the footnotes are from the FDIC article http://www.fdic.gov/consumers/consumer/idtheftstudysupp/part2.html

[3]FFIEC, "Authentication in an Internet Banking Environment." http://www.ffiec.gov/pdf/authentication_guidance.pdf

[4] Layered security refers to the layers of risk, from low to high, as well as the layers of authentication implemented, from weak to strong. Layers of authentication processes are matched with corresponding layers of risk.

[5] (This footnote is from the FDIC article, "Online Delivery of Banking Services: Making Consumers Feel Secure.") See "Industry Initiatives" at the end of this article for examples of industry initiatives targeted at deterring Internet theft and fraud, including the implementation of multifactor authentication procedures.

and security procedures on their own initiative in advance of the FFIEC letter and a number are working to meet the recommendations. During the same time as the discussion of these modest improvements in identity related functions there has been continued substantial growth in thefts and frauds on consumer accounts and a severe compromise of a much higher quality biometric-based three factor system implemented for bank executives.

The problems exacerbated by performing identity functions badly do not disappear when identity functions are done well. There is no point at which the security issues, identity crimes and other identity functions are solved. There will be criminals for the foreseeable future who search for and find ways to compromise electronic systems. This will entail continuing efforts to improve processes and technologies to fight the criminals, terrorists and others.

Many in the current generation having grown up with the Internet and its online communities where few or no rules of behavior exist, share and exhibit, often unwittingly, their most intimate personal information with the entirety of the virtual world. Once these details find their way to the Internet there is little that can be done to prevent their misuse or assure their removal. This generation of users will likely have very divergent attitudes toward sharing and providing personal information, or suffering through identity proofing processes and authentication requirements. Some will internalize an expectation of providing identifying information, having done so many times they will see no need to protect such information. Others who have suffered indignities or worse from the sharing of personal details may well react very negatively and push for government limitations or protections. These attitudes will no doubt vary from those of the prior generations that are coming to grips with the new rules or lack thereof in the virtual world.

The Challenge is Huge

Tremendous issues remain to be resolved. Hundreds of billions of dollars are spent and/or lost performing identity related functions as we do now -- which most often is poorly. Whether poorly performed or not, the costs of current practice are built into business methods through higher credit costs, charge backs to retailers, higher retail prices, risk management strategies and various other mechanisms that address and frequently hide the costs from sight. The problems are misunderstood and attitudes concerning the issues vary widely. This will make change difficult. Poor performance is not necessarily due to lack of concern or intent on the part of those implementing the systems but because there is no simple, straightforward answer. Our culture underestimates the value of or even fears doing these functions well, decision makers underestimate associated risks and a vocal minority misinterprets and sometimes misrepresents the issues. A tremendous effort will be required to change the culture, the systems, mechanisms and cash flows from their current paths and procedures.

***This Section is taken from the FDIC website:**
http://www.fdic.gov/consumers/consumer/idtheftstudysupp/part2.html

Indirect Costs
Direct cost estimates of identity theft have been criticized by some researchers as being too high,[9] but the indirect costs are widely considered to be undervalued. Indirect costs include slower adoption rates for online banking and bill paying and therefore

a greater use of more-costly banking channels; less effective Internet marketing efforts; loss of consumer confidence in online transactions inside and outside of banking; loss of faith in brand names; and increased concern about financial institution security more generally.[10] Costs resulting from publicity about identity-related security breaches include loss of brand equity, customer defections, lost business opportunities, costly litigation, and the cost of implementing better security.[11]

Measuring the concerns of consumers is one way of understanding the indirect costs of identity theft. Without question, retail consumers are concerned about identity theft and about the misuse of their personal information. Between one-half and three-quarters of U.S. households report that identity theft is a concern for them or that they are concerned about e-mail fraud. Internationally, some 80 percent of online adults worry about their online identity being stolen and used to access online bank accounts.[12]

Although consumers are worried about phishing and the trustworthiness of e-mail messages from their banks, they are also concerned about the security of their personal information more generally. Seventy-five percent of the respondents to one 2004 survey cited identity theft resulting from a security breakdown at the bank as a concern, up from 58 percent in 2003.[13] Consumers who bank online have expressed less confidence in the security of their personal information. When asked the question, 'are you as confident about the protection of your personal information when banking online as when you bank in a branch office,' consumers report a significant decline in confidence (from 74 percent in 2003 compared to 64 percent in 2004).[14] Concerns about fraud are subsumed within retail customers' varying levels of concern about how financial firms handle their personal information,[15] and merchants are concerned as well.[16]

Consumers are indicating that they may stop using or may refuse to adopt online banking because of their security concerns. Online consumers report that they agree with the statements that they will stop using (14 percent) or not enroll (20 percent) in online banking or bill paying because of concerns about phishing. Small business owners' reactions are similar.[17] Security remains a critical factor when a consumer is choosing a retail bank, and one-quarter of international consumers will be very likely to switch banks if, by doing so, they will have better identity protection.[18] One study revealed that two-thirds of respondents said they will switch banks if their bank fails to secure their personal information.[19] A small percentage of consumers—close to 6 percent—have even admitted to having already switched banks to reduce their risk of becoming a victim of identity theft.[20]

Although the costs to banks of consumer concern about security are substantial, the benefits of improved security are likely to be substantial as well. Improved security may open up new customer markets. Almost three-quarters of current Internet users who do not use online banking report that they will be likely to do so if identity security is improved. Of those that do use online banking, the vast majority report being willing to use more, higher-value services if their identities are better protected.[21] These issues have a far-reaching effect on the business of banking.

[9] For example, Robertson (2004) and Gould (2004).
[10] See Penn et al. (2005) and RSA Security (2003).
[11] RSA Security (2003).
[12] Louvel (2005), Penn et al. (2005), Graeber et al. (2004), Entrust (2005).
[13] Ponemon Institute cited in Nock (2005).
[14] Ponemon Institute (2005).
[15] See Penn et al. (2005), Graeber et al. (2004), and Entrust (2005).
[16] Almost half of online merchants are more concerned than in the past about online payment fraud, and two-thirds say that a higher incidence of identity theft is increasing the amount of online fraud. See CyberSource Corporation (2005).
[17] Penn at al. (2005). See also Graeber et al. (2004).
[18] Entrust (2005).
[19] Ponemon Institute cited in Nock (2005).
[20] Louvel (2005).
[21] Entrust (2005).

Identity, Access, Privacy and the Impact of Legislation

It is worth reproducing a quote from the previous EC3 paper on Identity Infrastructure:

> "More than a century ago Supreme Court Justice Louis Brandeis, perhaps best known for his ardent defense of the 'right to be let alone,'" (from which much of our privacy legislation bloomed), "also argued that '[i]f the broad light of day could be let in upon men's actions, it would purify them as the sun disinfects.' He proposed a 'companion piece' to his influential *Harvard Law Review* article, 'The Right to Privacy,' on 'The Duty of Publicity.'"[6]

Public access to government records, activities, proceedings and information on activities of members of the public serves several different and overlapping policy goals. Our society derives tremendous benefits from broad access to a wide range of public records. Our system of government depends on the oversight facilitated by open records and our financial system is built on the ready and open access to public records. Citizens need government information to make political decisions about government programs, legislative and regulatory options, and candidates running for office. Knowledge about government is an important element in instilling confidence in the political system. Citizens need government information to assist in oversight of and accountability for government programs. Individuals need government information to know what services are provided by government. Government information is a valuable resource and commodity that can be used in many different ways to further economic growth. Information about public activities helps, to paraphrase Justice Brandeis, to purify men's actions. It is likely to have similar effect on women's actions. However, there are other interests and values that may be negatively affected by the public availability of government information, and most cases call for a balance of conflicting interests. Government records may need to be withheld from public disclosure to protect state and national defense interests, to foster law enforcement investigations, to support the deliberative processes of government, to protect the confidentiality of private business information, and to protect the privacy interests of individuals.

Access to public records is not simply a yes-no proposition. Mechanisms to ensure the appropriate balance between disclosure and non-disclosure must be implemented both through legislation, policy, and procedure. The development of the identity infrastructure should at minimum include the capability to meet privacy requirements. This will likely mean controlling data access to the field level, logging access events and informing data owners of access events.

There are several good resources for information and perspective on privacy principles and protections. Following are two good sources: The Center for Democracy and Technology and Daniel Solove Publications. One of the best resources on the value of open records and access to information is The Coalition for Sensible Public Records Access found at CSPRA.ORG.

Government Agency Privacy Considerations

How government manages its stewardship of personally identifiable information (PII) is of much concern to some U.S. citizens. Resultantly, personal privacy concerns have been the topic of several Government Accounting Office (GAO) reports, with Congress expressing a specific interest in understanding how agencies are gathering and using personal information. A GAO report to the U.S. Senate, prepared May 2004, detailed over 199 data mining efforts (both planned and operational)

[6] Fred H. Cate and Richard J. Varn, *The Public Record: Information Privacy and Access—A New Framework for Finding the Balance* (1999) (http://www.cspra.org/csprasite/pdfs/thepublicrecord.pdf).

spread across 52 different Federal agencies. Of these efforts, 122 involved the use of personal information retrieved from both public and private sources – many to detect fraud, waste, and abuse.[7]

A more recent GAO report performed in 2006 examined agency purchase of personal data from information resellers, or knowledge brokers. This report stemmed from concerns raised by Congress resulting from several very public security breaches at reseller services. As a part of this examination, GAO reviewed how this personal data was handled by the agency. Their report findings reflected that agency practices for handling personal information received from information resellers was not always consistent with the Fair Information Practices or Privacy Act of 1974.[8]

Both reports indicate an increasing trend by Government agencies to use citizen personal data to meet mission goals, however the reader can also infer that a possible disconnect exists in how the data received from commercial services is treated when compared to data personally collected on individuals by the agency. This inference is supported through the many citizen and privacy advocate groups that have viewed the procurement of personal data from information resellers as Government's circumvention of the personal protections afforded by the Privacy Act. In a statement introducing proposed personal data privacy the Senate Judiciary Committee's ranking member, Senator Patrick Leahy, stated "We are living in a world where the government is increasingly looking to the private sector to get personal data that it could not legally collect on its own without oversight and appropriate protections."[9]

Established as a law by Congress in 1974, the Privacy Act provides American citizens with a greater say in the way that agencies maintain records about them and ensures that Government cannot maintain secret records or secretly disclose data to others about them. Inadvertent violations to the Act occur when agencies do not properly identify, label or handle personally identifiable information. Of more recent concern, as evidenced in these GAO reports, is the manner in which agencies have been gathering information from contracted commercial services. If not implemented correctly, use of these services could be construed as violating one of the Act's principal elements, conditions of disclosure, which states:

> "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains".[10]

To prevent disclosure, agencies must be careful to craft queries that do not provide commercial services with citizen data they do not already possess. This may mean that, instead of using a citizen's last name, first name and full Social Security Number (SSN) in a query to a service, the

[7] U.S. Government Accountability Office (GAO). May 2004. "Data Mining: Federal Efforts Cover a Wide Range of Uses". Retrieved from http://www.gao.gov/cgi-bin/getrpt?GAO-04-548.

[8] U.S. Government Accountability Office (GAO). April 2006. "Personal Information: Agency and Reseller Adherence to Key Privacy Principals". Retrieved from http ://www.gao.gov/new.items/d06421.pdf

[9] Senator Leahy. Quoted from the "Statement of Senator Patrick Leahy On The Introduction Of The Specter-Leahy Personal Data Privacy and Security Act of 2005." June 29, 2005.

[10] THE PRIVACY ACT OF 1974. 5 USC § 552a. As Amended. www.usdoj.gov/foia/privstat.htm

agency should craft the query such that either only the SSN is supplied without other personal identifiable data or, if a name and other information must be provided on the query, the query should truncate the SSN to use only the last four digits.

SSNs are viewed as the "Holy Grail" by most commercial data resellers as they are the most difficult for the service to harvest from public records. While eliminating the SSN or truncating it may somewhat reduce the matching ability of the service, it ensures that the agency is in compliance with the "conditions of disclosure" principal by not affording the commercial service with the ability to add the citizen's data to its own repository and, in turn, re-sell the data to other entities.

A U.S. Census Bureau study designed to assess the public's attitudes on privacy and confidentiality issues demonstrated increasing levels of disapproval towards the sharing of personally identifiable data and, specifically, to providing SSN information to government agencies (the survey involved data provided to the U.S. Census Bureau).[11] In light of recent agency data loss of personally identifiable data for millions of individuals over the last couple of years by several agencies, citizens are not presently viewing Government agencies as good stewards of personal information. Agencies must change this perception through the implementation and enforcement of strong privacy and data security policies, through educating agency personnel through data handling training, and by providing full disclosure to the citizen within the agency's privacy policies.

As requirements for strong identity proofing increase as a result of HSPD-12[12] and the Real ID Act, it is expected that Federal and State agencies will significantly increase the amount of personal data collected and stored from various sources. Agencies must be watchful that sufficient due diligence is applied to protect the citizen no matter what the collection method used.

Egregious Compromises

Since ChoicePoint first broke into our collective conscience in February 2005, egregious compromises of personally-identifiable data have been reported in the news with such regularity that many of us now take these compromises as a matter of course. One group that monitors such compromises is the Privacy Rights Clearinghouse, which maintains a website at http://www.privacyrights.org/ar/ChronDataBreaches.htm devoted to these incidents.

As of August 2006, the Privacy Rights Clearinghouse listed a total of 275 breaches. Of these, academic institutions such as colleges and universities formed the largest group of participants; 88, or 32%, of the listed breaches involved one of these institutions. One of the largest academic compromises occurred when Miami University accidentally posted approximately 21,000 student records online. That is hardly surprising, given the current perception of academic network security.

What is more surprising is that the second largest group is composed of financial institutions, which account for nearly ten percent of the total number of compromises. What these institutions lack in

[11] U.S. Census Bureau. "Census 2000 Synthesis Report No. 19: Results from the Social Security Number, Privacy Attitudes, and Notification Experiment in Census 2000". Issued March 2004. Retrieved from www.census.gov/pred/www/rpts/TR19.pdf.

[12] Information retrieved from the Office of Management and Budget's web site at http://www.whitehouse.gov/omb.

number of compromises, they make up in volume of customers affected. Financial compromises often involve lost backup tapes, such as the lost tape(s) belonging to Bank of America, which contained information for 1.2 million customers, and to CitiFinancial, which contained account information for 3.8 million customers. The clear winner of the award for the largest breach at any financial institution, however, is the now-defunct CardSystems, victimized by hackers who compromised up to 40 million customer accounts. MasterCard and American Express accused CardSystems of lax security practices and severed relations with CardSystems as soon as was decently possible. Visa extended its relations until CardSystems was purchased by another company and disappeared into oblivion four months after the breach was made public.

Not every mega-million-user compromise is followed by the disappearance of the victimized institution. In May 2006 the Department of Veterans Affairs revealed that a laptop containing personal information on 28.6 million veterans and their family members had been stolen from the home of an employee. The VA took a number of steps to address the issue, including penalizing the employee and recovering and analyzing the laptop. VA was eventually so reassured by its progress that it rescinded its offer of free credit monitoring to the victims of the compromise. Another federal agency, the Department of Education, accidentally exposed the information of as many as 6.4 million student loan recipients to other borrowers. It is unknown how many users actually took advantage of this vulnerability, or even if any ever did. Fortunately, neither of these venerable federal agencies is likely to suffer the fate of CardSystems anytime soon.

Retail outlets have also contributed their efforts to the compromise of customer data. The credit card database of Designer Shoe Warehouse, better known as DSW, was hacked to expose 1.4 million credit card accounts. The Federal Trade Commission accused DSW of exposing customer data to unnecessary risk. In an agreement to settle these charges, DSW agreed to implement comprehensive security controls, to be audited by an external auditor every other year for 20 years, and to allow the FTC to monitor compliance.

BJ's Wholesale Club found itself in similar hot water with the FTC. According to the FTC's press release:

> "…fraudulent purchases were made using counterfeit copies of credit and debit cards used at BJ's stores, and that the counterfeit cards contained the same personal information BJ's had collected from the magnetic stripes of the cards. After the fraud was discovered, banks cancelled and re-issued thousands of credit and debit cards, and consumers experienced inconvenience, worry, and time loss dealing with the affected cards. Since then, banks and credit unions have filed lawsuits against BJ's and pursued bank procedures seeking the return of millions of dollars in fraudulent purchases and operating expenses. According to BJ's SEC filings, as of May 2005, the amount of outstanding claims was approximately $13 million."

BJ's made a deal with the FTC similar to DSW's, including auditing and monitoring for 20 years to come.

Both public and private institutions have begun to look for scapegoats when compromises occur. In late July 2006, AOL posted, on a public web site, data on 20 million web queries from 650,000 users. Some search records exposed SSNs, credit card numbers, or other pieces of sensitive information. The CTO and two other employees left the company shortly thereafter.

Some compromises of customer data are intentional. Private institutions have complied with a growing number of federal demands for customer information without the benefit of an order from a court of law. Notably, AT&T, Verizon, and Bell South are reported to have furnished the National Security Agency with what one person called "the largest database in the world" of telephone calls and Internet traffic patterns of domestic and international origins. One estimate of the size of the database reached 1.9 trillion records. There is some dispute about the contents of these records, but the likelihood is strong that they contain phone numbers or other information that can be aggregated with other databases to identify individual customers. Lawsuits have been filed in at least four states by those who perceive themselves compromised by unlawful disclosure of their data.

One such settlement has already been won by privacy advocates. According to the website of the Electronic Privacy Information Center, Fidelity Federal Bank and Trust Co. in Florida purchased 656,600 names and addresses from the Florida DMV for use in direct marketing. According to the brief,

> "Florida failed to change its state law in 1999 to reflect Congress' strengthening of the Drivers Privacy Protection Act. As a result of this and other failures to secure personal information, there are many commercial databases available on Florida residents that are not available in other states."

In a class-action settlement, Fidelity Federal was required to pay $50 million to those compromised.

Dozens of the incidents listed by Privacy Rights Clearinghouse involve lost or stolen laptops, including the VA compromise mentioned earlier, but the number of unsecured laptops containing sensitive information remains another threat to data security. Computerworld magazine reported results from a survey released[13] in August 2006 by Ponemon Institute LLC and Vontu Inc., a San Francisco-based provider of data loss prevention products. Of approximately 500 information security professionals who were polled, over 80% reported the loss of one or more laptops containing sensitive information during the last year. Another 64% of those surveyed reported that they have never conducted an inventory of their company's sensitive information or taken an inventory of employee data. Participants in this survey have not begun to identify or protect their sensitive data, indicating that it may be some time before any reduction of the incidence of data loss through loss of unsecured laptops.

The report of the ChoicePoint data breach was one of the first and most notorious reports of data compromise, and it was precipitated by the California state law requiring organizations to notify customers whose data may have been compromised. Based on the evidence of the intervening months, the only thing that is likely to end the current flow of breach reports is the passage of federal legislation removing the state-level requirement for companies to report these incidents.

Management of "Breeder Documents"

[13] http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/08-15-2006/0004416275&EDATE=

Compounding the issues of privacy is the notion of publicly accessible records. Currently, an individual's identity is based on what are termed breeder documents. Breeder documents include those government records establishing the rights of the citizen as a citizen of the county, state, and country – records of vital events, employment applications, drivers' licenses, voter registration records and student academic records to name a few. Directly or indirectly the initial information about an individual begins with birth. This generally means a birth certificate or baptismal record. Since those documents were not designed to serve the requirements of identity, but rather those of vital statistics they are not very secret nor all that secure. Records of vital events – birth, death, marriage, divorce – are widely and readily available at both the county and state levels. Walk in to most state archives in this country and with minimum identification, anyone can access vital events records that have been determined historical – usually 100 or more years old. The security procedures are designed to protect the record itself, not the identity embedded within it. That vital event record, that birth certificate, is the "key" to unlock the door of identity. A birth certificate can be used to obtain a driver's license and in turn most other credentials in this country. A tremendous challenge in moving forward will be to address the protection of breeder documents that establish citizenship and identity.

Looking Toward the Future

There are years to come in which expenditures will need to dramatically increase to make up for under spending in the past. During this period there will continue to be dramatic breaches and compromises of personal information. Some of the results will be disastrous for businesses, leading to bankruptcy or dissolution, and very damaging and embarrassing for government organizations, managers and elected officials. Tens of millions of Americans will be affected by identity related crimes and hundreds of billions of dollars lost. These numbers will continue to increase on an annual basis unless the resources expended in time and funding rise to a level necessary to reduce the underlying rate of crime.

The next few years will witness a wide disparity of spending to perform identity functions. There will be continued development of application-based IDM and access control. Parallel to these developments will be movements to consolidate functions at other levels of the organization, across systems, division, agency and enterprise. During the upcoming several years the costs and difficulty of performing a particular identity function or number of functions will moderate as techniques and technology are created and improved. Use of these will become more widespread, and services and offerings will be developed to meet these needs. These moderating costs may not seem apparent to many application or system owners who have not performed sufficient IDM functions nor resourced at an appropriate level.

Governance will become a big concern as identity functions are performed across a wide range of boundaries including government at all levels and throughout the non-government portion of U.S. society. Making decisions and committing to the deployment of resources across such a range of boundaries will exacerbate existing issues and create new ones. A variety of laws and rules will be passed in reaction to continuing crimes and concerns. While generally well-intentioned, past experience suggests that a patchwork of inconsistent or incompatible legislation is the likely result and may well have the unintended effect of making the attainment of goals more difficult or impossible.

Identity Infrastructure of the Future

Development of Identity Infrastructure will continue. New identity federations will continue to grow and existing federations will expand the scope of users and uses. Policy work will continue through such groups as the E-Authentication Partnership. The EAP has undertaken the task of creating a policy framework that allows the use of credentials across a range of relying parties including application owners, organizations or federations. It has begun work on accrediting assessors of participating organizations. Participating organizations are sharing lessons learned from building and operating federations to extend and expand the benefits of participation to new organizations.

Interoperability is vital to the functioning of an infrastructure. Imagine if every plug-in for electrical power (think of your laptop) and the voltage sent down each line was different. It would severely limit the adoption and usefulness of electrical power. If you have had to replace a power cord for your laptop you have some idea of just how valuable interoperability can be. Similarly, if the components of the identity infrastructure do not seamlessly interoperate then adoption will be slow and use will be difficult.

A lot of policy, procedure and technology must be developed to bind the components of an identity infrastructure together. Attitudes towards and practices for the protection of personally identifiable information must be changed to protect breeder documents and to establish codes of behavior with regard to providing such information. Methods will also be created to build upon existing components to create better or stronger identity functions without redoing previous work. A preexisting credential could serve as evidence that certain steps were completed and do not need to be performed again.

Business model(s)

A big hurdle still to be faced is creation of a business model that will support development, operation and maintenance of the identity infrastructure and its components. There is substantial agreement that there is value to building an identity infrastructure. One problem to overcome is who will pay and how. There are a variety of possible business and organizational models that should be considered to meet a wide range of needs and to reconcile seemingly incompatible requirements. Follows are some suggestions for consideration:

- Public-private partnership
- Non-profit organization
    - Private
    - Government chartered
- Fee for service
- Subscription
- Government funded
- Cost or loss reduction sharing
- Loss recovery sharing

There are no doubt many more innovative possibilities if certain hurdles such as liability can be overcome.

Liability

A very serious issue is liability. There are large and frightening questions of liability for any in the private sector who attempt to build solutions or components of this identity infrastructure. Imagine if a business developed a service that performed identity verification and issued credentials, those credentials were trusted to permit access to transportation systems. Imagine further that someone using one of those credentials boarded an airplane and committed a heinous act that killed thousands of people. It may not be very likely that the credential issuer would lose a lawsuit arising out of such an occurrence, but it is likely that it would be involved in one. It is this potentially huge unknown that repels many possible solution providers. Questions of legal liability, who pays and how much, are largely untested by courts. A number of potential business models will be forestalled by legitimate fear of potential liability.

Participation

Participation will take on numerous forms as components become interoperable and systems use state of the art methods to "connect" with others. Individuals will "enter" the identity infrastructure from a variety of portals. Some times it will be as a result of employment. Doing work for the federal government requires a Personal Identity Verification (PIV) card. Most Americans will receive a Real ID. Health consumers may soon receive a credential from a health provider. As the infrastructure is developed these credentials will be accepted at a widening array of online and inline points of access to perform a growing number of interactions and transactions.

Coming Attractions

For an identity infrastructure to be successful, an identity system or process of establishing identity must be developed. Although the first steps are in process this country has not created an identity system so there is no good point of origin, no starting point, for identity. Today all identity verification starts with something the person knows-- directly or indirectly that initial knowledge usually relates to birth. Since vital events records – birth, death, marriage, and divorce -- are not designed to serve the requirements of identity, but rather those of vital statistics they are not very secret nor all that secure. The information on births is widely and readily available and security procedures for obtaining birth certificates range from non-existent to moderate *as intended for the vital statistics uses.* It is generally the information pertaining to a particular birth that is the key to obtaining that particular birth certificate. That birth certificate is the "key" to unlock the door of identity. Once an individual secures a birth certificate, most other credentials, such as a driver's license, can easily be obtained. This type of knowledge-based verification creates a less than firm foundation for any successful identity infrastructure. Addressing this and other issues will be vital to moving forward.

Knowledge-based Verification and Authentication-The Decline and Fall

Knowledge is currently used to both verify identities and to authenticate individuals. The use of knowledge to perform these functions is based in concept on the knowledge being secret or difficult to access, available on a desired population and readily accessible to those performing these functions. These very requirements that make the information worth using make it of limited long term use. These requirements to some extent are mutually inconsistent, access to these information sources is relatively easy and there are few sets of information that cover large proportions of the population. Simply stated the use of knowledge for verification and authentication rapidly destroys its value for these uses.

Additionally, using personal information exacerbates the very problems that a system employing this information would be attempting to prevent. Spreading use of personal information for verification and authentication heightens the likelihood of the information becoming compromised. The use of knowledge for these functions will likely be of relatively short term use. Other methods will need to be developed to take their place.

Identity Hardening

There are some options developing that may replace or at least supplement knowledge-based authentication. The first lacking a good title can be described as identity hardening. Conceptually, identity hardening involves creating an ever harder "shell" around a core identity. The core may well an identity verification that is performed in whole or in part through use of knowledge held by the individual, but that knowledge would not be used for authentication purposes. Devices, one-time passwords, biometrics or other factors substitute for "something the user knows." As requirements grow for higher levels of security and authentication the identity is hardened by performing additional verification steps and strengthening methods of authentication. It is likely that the developing identity infrastructure will foster a trend toward identity hardening as more valuable and riskier transactions and interactions are contemplated.

Internet Identity

This is a very new effort to create identity verification and authentication processes and technology using open source techniques. There is relatively little information available at this time, but this effort is worth monitoring as it is gaining the attention of very good people and organizations. The announcement of the upcoming meeting can be found at this web address: http://www.windley.com/events/iiw2006b/announcement.

Standards of Identity

Lots of standards have been developed and are in process. An effort is underway through a collaboration of the American National Standards Institute and the Better Business Bureau to collect and catalog existing standards entitled the Identity Theft Prevention and Identity Management Standards Panel. More information on standards is available in the 2006 EC3 document, Technology of Identity.

Technology of Identity

The EC3 formed a workgroup this year 2006 to gather information on the Technology of Identity so this topic will not be covered extensively here. There is a technological development worth noting in the context of the developing identity infrastructure. Current state of the art authentication involves three-factor authentication, something you (the user) has (a token), something you know (a password), and something you are (a biometric). Technology is under development to perform multi-factor and variable factor authentication. There are numerous other factors that are likely to be developed to augment authentication. Some of which will included expanded use and types of knowledge, user location and system information or multiple biometric indicators. Variable factor authentication is the use of a changeable set of factors. These could be drawn from previous transactions or more limited data sets and would help to increase the difficulty of compromising the system.

Conclusions

Over the past three years there has been a significant amount of work accomplished, but in some sense it seems that there is more to be done than in 2003. This is a result of better understanding of the overall problem to be solved and much more detailed work having been accomplished. It may well be that in another three years this sense if repeated as there is much more work still to be done and a long way to go. Nationwide infrastructures take a long time to develop. Their timelines are measured in decades as will this one be.

Many of the needed efforts are underway or in development. Standards are being developed, policy and procedures are being created, technology is adapting and being deployed. There are still some significant issues to be resolved as follows:

- Governance--the activities to be governed take place in both the real and virtual worlds and cross traditional government boundaries at the speed of light. The participants adapt in "real-time" so decisions and changes must be made at a similar rate. This is a new infrastructure in a new environment and old methods of governance and decision making processes will likely not be effective.
- Business Model—there must be created a system for appropriately funding the needed upfront investment and ongoing operations for this identity infrastructure. This means that someone will pay. We all already do pay—a lot—for doing these functions badly. A successful business model will likely involve a variety of mechanisms, government and private investment, fee for service, shared savings and/or micro payments, cobbled together to reach an eventual stable operating state.
- Liability—without the mechanism of liability then users of a system have little to gain by participating. If their potential losses are not covered then there is severely limited value for individual users or relying parties in using the infrastructure. If liability in its current unbounded form is included then it verges on impossible to create a sustainable business model. Some compromise will be needed which will either use government protections or some other mechanism to mitigate the current boundless nature of the risk to providers while providing the worthwhile incentives of liability.
- Privacy/Openness/Information Use—there are open issues to be addressed. Building this identity infrastructure is changing the nature of personal information flow and use. Operation of the infrastructure requires an ocean of personal information. Such an ocean has vast currents, its own ecosystem and is very difficult to contain. This country is at a decision

point. Will we as a society take on the task of designing the ecosystem and determining the flow of the currents or will we leave these to be determined by a somewhat “unnatural” selection.

We will check back in a few more years.