INSCT
INSTITUTE FOR NATIONAL SECURITY AND COUNTERTERRORISM
SYRACUSE UNIVERSITY

Jointly sponsored by
Syracuse University's
College of Law and
Maxwell School
of Citizenship and
Public Affairs

September 20, 2010

The Honorable Gary Locke
Secretary of Commerce

Patrick Gallagher
Director, National Institute of Standards and Technology

Francisco J. Sánchez
Under Secretary of Commerce for International Trade, International Trade Administration

Lawrence E. Strickling
Assistant Secretary for Communications and Information, National Telecommunications and Information Administration

via email to cybertaskforce@doc.gov

Re: Cybersecurity, Innovation and the Internet Economy
Docket Number 100721305–0305–01

Dear Secretary Locke, *et al*.:

Please find attached comments submitted in response to the Notice of Inquiry (NOI) on Cybersecurity, Innovation and the Internet Economy issued by the Department of Commerce and published at FR Doc. 2010–18507.

We submit that only an interdisciplinary approach can meet the challenges raised in your notice of inquiry. Thus, the attached comments were developed by a panel comprised of professors from six academic disciplines within Syracuse University as well as practitioners from the business community.

We would be pleased to provide additional information upon request.

Sincerely,

William C. Banks
Director, Institute for National Security and Counterterrorism

Shiu-Kai Chin
Director, Center for Information and Systems Assurance and Trust

Comments on Cybersecurity, Innovation and the Internet Economy

Submitted by the Institute for National Security and Counterterrorism
and the
Center for Information and Systems Assurance and Trust
Syracuse University
September 20, 2010

The following comments are submitted in response to the request for comments contained in the Notice of Inquiry (NOI) on Cybersecurity, Innovation and the Internet Economy issued by the Department of Commerce and published at FR Doc. 2010–18507. More specifically, these comments address questions four and eight posed in the NOI concerning "Authentication/Identity (ID) Management" and "An Incentives Framework for Evolving Cyber-Risk Options and Cybersecurity Best Practices."

The Institute for National Security and Counterterrorism (INSCT) and the Center for Information and Systems Assurance and Trust (CISAT) jointly conducted a roundtable discussion on these topics by a panel of experts. Included in the discussion were:

- Professor William C. Banks of the College of Law and the School of Citizenship and Public Affairs;
- Dr. Glenn Benson, Security Architect, Treasury Services, JP-Morgan Chase[*];
- Professor Shiu-Kai Chin of the Electrical Engineering and Computer Science Department;
- Mr. Sean Croston, Vice President, Sr. Product Manager, JP-Morgan Chase[*];
- Professor Lisa A. Dolak of the College of Law;
- Professor Kevin Du of the College of Engineering and Computer Science;
- Dean Randy Elder of the School of Management;
- Professor David M. Rubin of the School of Public Communications;
- Professor William Snyder of the College of Law;
- Dean Jeffrey M. Stanton of the School of Information Studies.

Biographies of the participants are contained in Appendix II. Video and audio of the complete roundtable discussion can be found on the World Wide Web at http://insct.syr.edu/insct_events.aspx?id=36507230109 .

[*] Dr. Benson and Mr. Croston participated in their personal capacities and not as representatives of JP-Morgan Chase. None of these comments should be attributed to them or to their employer.

There is, as yet, no national cybersecurity policy. Such a policy is a necessary step to secure the interests of the United States in cyberspace. The Obama Administration released a draft National Strategy for Trusted Identities in Cyberspace (NS-TIC), to be finalized in the fall of 2010. The panel views the NS-TIC to be a component of and a progressive step towards a comprehensive national cybersecurity policy. The panel convened specifically to assess that draft NS-TIC and, ultimately, to offer recommendations for specific parts of that strategy. To be accurate, comprehensive and effective, such an assessment must be interdisciplinary in nature.

The draft NS-TIC offers four guiding principles, four goals and nine high-priority actions, as detailed in Appendix I of these comments. Privacy, accountability, and technical protocols and interoperability are three topics that cut across these principles, goals, and actions. Resolution of these issues requires input from practitioners and experts in multiple disciplines including law, computer engineering, public policy, and information science.

Topic 1: Privacy

The use of strong identification by all actors on the Internet would make the cyber realm sufficiently trusted for commercial activities and make it much more difficult for criminals and terrorists to operate with impunity. At the same time, it would far more than simply risk chilling free speech; in many countries the government could use the identification data to literally kill dissent. This conflict was displayed when U.S. Secretary of State Clinton stated:

> [O]nline organizing has been a critical tool for advancing democracy and enabling citizens to protest suspicious election results. … The freedom to connect to these technologies can help transform societies …. The United States is committed to devoting the diplomatic, economic, and technological resources necessary to advance these freedoms. … [T]he State Department is already working in more than 40 countries to help individuals silenced by oppressive governments. We are making this issue a priority at the United Nations as well, and we're including internet freedom as a component in the first resolution we introduced after returning to the United Nations Human Rights Council. We are also supporting the development of new tools that enable citizens to exercise their rights of free expression by circumventing politically motivated censorship.

Yet, in the same January 21, 2010, speech, the Secretary explained:

> [W]e must also grapple with the issue of anonymous speech. Those who use the internet to recruit terrorists or distribute stolen intellectual property cannot divorce their online actions from their real world identities.

Clearly, both providing strong identification and limiting a company or government's ability to demand that an Internet user provide that identification will require massive government effort, regulation and policing in the cyber realm. Is that possible? Is it wise? If so, how best to do it?

One of the four Guiding Principles of the draft NS-TIC states that identity solutions will be "privacy enhancing." People do use the Internet for private communications or to visit web sites with which they would not wish to be associated publicly. On the other hand, many times people want their online activities such as posting an entry on a news or political blog to be very public, but they desire to remain anonymous. Anonymity may promote free speech and political dissent, but it makes attribution of responsibility for nefarious activities very difficult. How can anonymity and security best be balanced, and by whom?

Dean Stanton notes that privacy is a social good, particularly in a democratic society, but privacy is one of multiple goals that the draft strategy attempts to promote. As noted in the previous paragraph, these goals may conflict and result in an over-constrained system that might be extremely difficult to achieve. Stanton suggests considering what the NS-TIC is attempting to accomplish and then focusing on just one point.

1.1: Anonymity

The draft strategy "recognizes the value of anonymity for many online transactions (e.g., blog postings)" (p.1).[1] It claims that "The Identity Ecosystem also enables anonymity for individuals interacting with services that do not require strong identification and authentication" (p.12). The draft asks readers to imagine the optimal cyber identification environment:

> An individual voluntarily requests a smart identity card from her home state. The individual chooses to use the card to authenticate herself for a variety of online services, including:
>
> - Credit card purchases,
> - Online banking,
> - Accessing electronic health care records,
> - Securely accessing her personal laptop computer,
> - Anonymously posting blog entries, and
> - Logging onto Internet email services using a pseudonym.

(P.4.)

Would such "anonymously post[ed] blog entries" that required authentication via a smartcard really be anonymous? The NS-TIC defines the word "anonymous" as: "Not named or identified.

[1] Unless otherwise indicated, all citations are to the page number of the *National Strategy for Trusted Identities in Cyberspace: Creating Options for Enhanced Online Security and Privacy*, June 25, 2010, available at http://www.dhs.gov/xlibrary/assets/ns_tic.pdf (last visited Sep. 17, 2010).

Anonymous transactions allow for information exchange between parties without the need to identify the parties involved" (p.32). The identity provider -- in this example, a government -- certainly does know the identity of the "anonymous" poster or the person "logging onto Internet email services using a pseudonym." The definition is only accurate if it is appended to read "without the need to identify the parties involved *to the parties involved*." Other parties certainly will know. The identity provider and the service that authenticates that identity to permit it to post anonymously will know the actual identity of the individual. Even when the identity provider is not a government, its records will have little Constitutional protection from government acquisition under the third party records doctrine.[2] Thus, many real world blog posters already have criticized the NS-TIC as an attempt to positively identify blog posters and people who use pseudonyms for email addresses. Critics rephrase the preceding paragraph as the government saying: "Let me give you a smart card so that we will know who you are when you post anonymously." A July 2, 2010, *New York Times* headline described the strategy as "Taking the Mystery Out of Web Anonymity." You might be anonymous to the person with whom you are communicating, but you will not be anonymous to the government. Professor Du, on the other hand, has done research on privacy preserving computation. He notes that this seeming contradiction – obtaining a credential to be anonymous – is not necessarily impossible, and he generally supports the draft NS-TIC and its call for the development and use of new technology.[3]

The draft NS-TIC calls for the Federal Government to "create action plans to strengthen privacy" to:

- Limit collection and transmission of information by Identity Ecosystem participants to the minimum information necessary to fulfill the purpose of the transaction.
- Limit secondary uses of individual data collected and transmitted in the Identity Ecosystem.
- Limit retention of data to the period necessary for the provision of the services to the individual end-user for which the data were collected, except as otherwise required by law.
- Minimize data aggregation and linkages across transactions in the Identity Ecosystem.

(P.28.)

Current limitations to the retention and dissemination of wire, oral and electronic communications (all terms with specific legal definitions) are found in the Electronic

---

[2] Current Supreme Court doctrine is that the records of a third party such as a bank or telephone company belong to that party. The person about whom the records pertain does not have a Constitutionally protected interest in those records, although Congress can and sometimes has enacted statutes that provide additional protection.

[3] *See* Wenliang Du and Zhijun Zhan, *A Practical Approach to Solve Secure Multi-party Computation Problems*, New Security Paradigms Workshop, Virginia Beach, Virginia, USA. September 23 - 26, 2002.

Communications Privacy Act, the Wiretap Act, the Pen Register Act, and the Stored Communications Act. Those statutes apply to at least some of the proposed identity ecosystem participants, such as Internet service providers (ISP's). In highly abbreviated form, the current statutes limit providers to the public of "electronic communication service" or "remote computing service" (again, both specific legal terms) from voluntarily disclosing to the government information about their subscribers, such as physical world identities, sessions logs, IP addresses, and emails. Thus, the current approach to protecting the data delineated in the four bullet points, above, is to criminalize and to provide a private right of action for collections, retentions, disseminations and aggregations prohibited by acts of Congress. If the "action plans" to protect such data are to rely upon criminal and tort law, then these statutes will need to be modified and expanded. In addition, such regulation will require an enforcement mechanism, as discussed under Topic 2, below.

Professor Snyder challenges whether anonymity is a legitimate goal, or at least whether it should be given primacy. He notes that while surely free speech must be protected, the United States Supreme Court stated in 2010: "[D]isclosure requirements may burden the ability to speak, but they … do not prevent anyone from speaking."[4] Aren't people more likely to commit crimes when anonymous that they would not when known to their victims?

Professor Rubin argues that whether anonymous speech can be separated from free speech really depends upon the marketplace of ideas. In the United States we are still able to enter the marketplace of ideas (including that in the cyber realm) using our own names without fear of being rounded up by the government. People in many other countries cannot feel that way, however. Professor Banks questions how a U.S. policy might affect, for example, Iranian dissidents. Professor Snyder notes that if we attempt to accommodate both of the strains of the Secretary of State's speech quoted above, then we will need someone to monitor cyber traffic and determine what is protected political expression and what is not prohibited terrorism recruitment. Whom do we trust to do that? How do we define what is terrorism or child pornography? Typically, notes Dean Stanton, that determination is done by courts, but long after the fact according to Professors Dolak and Snyder.

1.2: Attribution

"Attribution" is a term not defined or used in the draft NS-TIC. Usually, it refers to determining the person responsible for a nefarious attempt to disrupt or alter a computer network or data. An American Bar Association report calls it "[a]rguably the most salient technical issue in Cyberconflict," and it is an obvious necessity for enforcement of laws against cyber crime. Of course, an action in cyber space that is truly anonymous is by definition incapable of attribution. Security requires a high capacity for attribution, while anonymity requires the opposite. Thus, the spectrum of attributability may be considered by some people to be a tradeoff between security and civil rights. Requiring the use of trusted identities for all actions in cyber space would make attribution easy and accurate but anonymity impossible.

---

[4] *Doe v. Reed*, 561 U.S. ___, Dkt. No. 09-559, 2010 (slip op. at 7).

1.3: Who strikes the balance

This tradeoff is seen in the Secretary of State's call to develop "new tools that enable citizens to exercise their rights of free expression" while at the same time pledging that "[t]hose who use the internet [sic] to recruit terrorists or distribute stolen intellectual property cannot divorce their online actions from their real world identities." Clearly, the Secretary wants persons engaging in political speech to be able to conceal their real-world identities from tyrants, but terrorists and criminals to not be able to do so. If persons use the same smartcard for banking, medical records and "anonymous" blog posts, their speech can be attributed to their physical world identity. Who will make this necessary balance between trusted identification and civil liberties?

Arguably, the draft NS-TIC attempts to let individuals strike this balance for themselves. "Voluntary participation is another critical element of this Strategy. Engaging in online transactions should be voluntary to both organizations and individuals," says the draft NS-TIC (p.13). This refers to two types of voluntariness. The first concerns which attribute provider a person uses. The second concerns whether a person chooses to participate at all. Individuals and organizations would be able to voluntarily choose which and how many identification providers with which to enroll, with options including both government and private providers. "Thus, the Identity Ecosystem should allow an individual to select the credential he or she deems most appropriate for the transaction, provided the credential meets the risk requirements of the relying party" (p.10). The draft strategy also envisions a voluntary choice about whether to participate in the trusted Identity Ecosystem at all. "Engaging in online transactions should be voluntary to both organizations and individuals" (p.13).

A counterargument questions whether such choices really can be voluntary. An individual's freedom to choose among credentials may have practical limitations based upon interoperability and the requirements of the other party. Also, regulation will affect the available options. An individual may wish to use a weak credential with limited data, but the vendor with whom she wishes to do business may be unable or unwilling to accept that credential. Also, the vendor may attempt to require more information than actually necessary for the transaction in order to, for example, target advertising, unless regulations prohibit and enforce limitations on demanding such additional information.

Freedom to choose whether to engage in online transactions at all also may be impractical. Legally, people are free not to have a telephone, but in reality it is very difficult to function in contemporary American society without one.

Moreover, the draft makes a fundamental assumption that voluntariness is a desired attribute of an identity ecosystem. Is that assumption valid? Another approach would be to develop a new Internet protocol that would require every packet of data to embed within it the user's authenticated identity. As a leading commentator noted: "It could stop most cyber crime, cyber

espionage, and much of cyber war."[5] Such a protocol is effectively a requirement to disclose a user's physical world identity.

Dean Elder and Dr. Chin note that private organizations such as Yahoo and Google right now are effectively performing the function of determining the balance between anonymity and authentication in the absence of courts. Professor Banks observes that historically, law has been behind. Judges seem loathe to understand technology and to make policy. Judges will do a poor job of making policy by cobbling together results of specific disputes when, as here, either the private sector or government should determine policy. This, asserts Banks, is one reason to be sympathetic to the effort by the White House to develop this draft NS-TIC; it moves these questions out into the public policy domain.

Various panel discussants note that American society is evolving its expectations of privacy. It is clear that under law there is no recognized expectation of privacy for acts committed in public view. Nevertheless, citizens are increasingly drawing distinctions between what they want to be private from government and what they want to be private from each other. Indeed, what people believe should be private – that is, not attributable or authenticatable by means of identity mechanisms deployed on the Internet – are culturally specific, rendering policy making for the World Wide Web especially difficult.

Topic 2: Accountability

One of the stated objectives of the draft NS-TIC is:

> Define participant responsibilities in the Identity Ecosystem and establish mechanisms to provide accountability.
>
> Key elements of the Identity Ecosystem Framework are defining the rights and responsibilities of the various participants in the Identity Ecosystem and establishing an enforcement mechanism, if participants do not carry out these responsibilities. …. Multiple entities currently enforce online security and privacy standards in a distributed fashion across both government and the private sector. Any new laws and policies must maintain the flexibility of this approach, while harmonizing a diverse and sometimes conflicting set of requirements that currently prevents interoperability and trust across communities.

(Objective 1.2, p.22.)

Some of these new laws would be the ones developed under Topic 1.1, above, to ensure privacy protections. Others laws, however, would need to establish the governance layer of the identity infrastructure itself. Three options for enforcement mechanisms include criminal statutes enforced in courts of law, regulations enforced through administrative proceedings, and private

[5] Richard Clarke, *Cyber War: The Next Threat to National Security and What To Do About It* (Harper Collins Press 2010) at 274.

rights of action for damages or injunctive relief. "The Identity Ecosystem Framework provides the overarching standards and laws that govern specific Trust Frameworks" (p.16). "[The Strategy] should also ensure that organizations limit data collection, only use and distribute information that is relevant and necessary, maintain appropriate safeguards on that information, and are responsive and accountable to individuals' privacy expectations" (p.9).

2.1: Regulating entities

In addition to such laws or regulations, the draft NS-TIC calls for the designation or creation of a governmental agency to oversee the identity ecosystem.

> **[High Priority Action] A1: Designate a Federal Agency to Lead the Public/Private Sector Efforts Associated with Advancing the Vision**
>
> …. The White House will select an agency and hold it accountable for coordinating the process and organizations that will implement the Strategy. Many other Federal agencies will have implementation responsibilities associated with their respective mission areas, and some of these are outlined in this document. However, the Lead Agency will:
>
> - Assess progress against the goals, objectives and actions stated herein;
> - Ensure the government leads by example in developing and supporting the Identity Ecosystem;
> - Coordinate collaboration and joint-owned actions across private and public entities, as they work to develop the Identity Ecosystem;
> - Support interagency collaboration and coordinate interagency efforts associated with achieving the vision; and
> - Establish private sector advisory mechanisms and engagement strategies.

(P.26.)

Although these proposed tasks include many that are persuasive in nature, "implementation responsibilities" would require an agency or agencies to participate in the development and enforcement of the new laws that establish the relevant rights and responsibilities.

Options to be designated as lead agency include, among others:

- Office of Management and Budget (OMB)
- Federal Bureau of Investigation (FBI)
- National Security Agency/Department of Defense (NSA)
- Department of Homeland Security (DHS)
- Department of Commerce (DOC)
- Federal Communications Commission (FCC)
- Federal Trade Commission (FTC)
- National Institute of Standards and Technology (NIST)

- The White House
- An entirely new agency.

Senate Bill 733, commonly known as the Rockefeller/Snowe Bill, would assign the Commerce Department lead agency responsibilities. Senate Bill 3480, Protecting Cyberspace as a National Asset Act of 2010, introduced by Senator Lieberman and reported out of committee on June 24, 2010, would designate the Department of Homeland Security as lead agency. Former Special Advisor to the President for Cyber Security Richard Clarke proposes creation of an entirely new Cyber Defense Administration.

The strategy's call to "designate a Federal agency" reflects a fundamental choice made by the as-yet-unknown drafters. Should the lead agency be a government agency? Should it be private or some type of hybrid, such as the Internet Corporation for Assigned Names and Numbers (ICANN) or the Internet Assigned Numbers Authority (IANA)? Professor Rubin notes that so far the NS-TIC leaves open the determination of the scope of the lead agency's responsibilities. For example, would it take over the trusted identity function of issuing passports that the Department of State now performs? Dean Stanton asserts that physical objects such as vehicle registrations and passports do not fit well within the cyber context. He suggests that there is, however, an interesting lesson to be drawn from the development of RFID (radio frequency identification) passports. It was a convoluted process that had many missteps in it, suggesting to some that government is not the best place to coordinate the development of a privacy protecting technology.

Dr. Chin doubts that the public will trust a centralized government agency. As evidence, he notes the experience in the 1990's with the debate over requiring providers of encryption or data transmission to provide a "back door" for government access[6] (as required by the Communications Assistance to Law Enforcement Act (CALEA)).

2.2: Civil Liability

The strategy concludes that in order to induce individuals and organizations voluntarily to participate, we "must address the liability concerns of service providers and individuals."

> This Strategy defines an Identity Ecosystem where one entity vets and establishes identities and another entity accepts them. To date, the appropriate apportionment of liability has prevented the cross-sector issuance and acceptance of identity credentials. The Federal Government must address this barrier through liability reform in order to establish the multi-directional trust required by transaction participants.

(P.28.)

---

[6] Steven Levy, *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age*, Penguin 2002.

Conceding that historically "*appropriate* apportionment of liability has prevented the cross-sector issuance and acceptance of identity credentials," how might the federal government reshape the liability environment to incentivize security practices without inadvertently punishing security providers for lapses beyond their control? Cyber insurance could be one method of apportioning liability, as could be caps or floors on liability for fraudulently used credentials.

Professor Dolak verifies that liability concerns have prevented some people and organizations from offering or using trusted identity services. The NS-TIC seems to contemplate a new legal framework, but she is pessimistic that such a legal framework can accomplish the draft strategy's objectives. Law tends to develop in reaction to events. Certainly the traditional court system reacts after things go wrong. That is by design. Civil liabilities compensate after someone has suffered a harm or loss. Even statutes tend to be the result of some perceived problem. Congress makes some fact-findings, and then issues a solution, often in result to an event featured in the news media. Professor Dolak disagrees with the draft NS-TIC's paradigm of an "ecosystem." An ecosystem, she asserts, is parts interacting with each other and evolving. The strategy envisions something set up ahead of time that works beautifully, inducing cyber actors to dive in and participate. That is just not realistic, she believes. We now have a patchwork of laws with significant limitations, and the relevant civil law is less developed than the criminal law is. Claims against an institution that loses private information such as credit card data tend to fail. As a society, we have not yet reached an agreement about the operable standard of care. What measures should be taken to protect electronic data? What standard of care is due? What claims are reasonable?

Dolak explains that another problem under civil liability law is that there is no recovery where there are no damages. Until harm is proven, there is no recovery when data is stolen. A lot of data breaches are unrecoverable under the eyes of law. Many times, she notes, there is not even evidence that such data is in the hands of someone who might want to do harm, as opposed to someone who obtained the data by accident. Even when an institution knows it has suffered harm and knows that there has been a data breach, often there is no proof that the breach caused the harm.

Private enforcement of liability is just one aspect of the civil legal framework. Another is government oversight. The agency in charge of overseeing data breaches is the Federal Trade Commission (FTC). It remains debatable, according to Dolak, whether the FTC has statutory authority in this area. Additionally, few, if any, FTC actions in this area have resulted in civil fines. In terms of government civil enforcement, the most effective security has come from interagency agreements. These take all kinds of forms. A classic example is that of VISA and banks capping losses to consumers. Professor Dolak sees the legal landscape developing not by virtue of government in place ahead of time, but by these kinds of private agreements that develop between parties. In the end, she argues, it will be self interest that provides the best protection.

Dean Elder reports that the business community would say that the government already is overreacting. Mandated solutions are costlier than the problem, especially given that some companies already move vast value through the cyber realm. Clearly, they must believe that they already have sufficient security and liability protection for what they already choose to do.

Dean Stanton is very alarmed that placing caps on liability now may distort a system that we do not yet understand. On the other hand, will businesses participate at all in an authentication system in which there are no limits whatsoever to liability for inaccurate authentication or for loss of the confidentiality of personal data?

2.3: Criminal sanctions

"The Identity Ecosystem may assist law enforcement in investigating **fraudulent activity that arises out of misuse of the system"** (p.20, emphasis added). No doubt, the widespread use of identity providers and of authentication would be enormously helpful to law enforcement. On the other hand, law enforcement can assist the Identity Ecosystem. Imposition of criminal sanctions for abuse or failure of the trusted identity ecosystem created by the National Strategy would help to ensure its effectiveness and that it achieves the trustworthiness required for individuals to choose to use it.

How best could the government use sanctions to promote trust and thereby induce people to obtain strong government-issued identification?

- By requiring it, like drivers' licenses, backed by civil sanctions or criminal punishment?
- By providing financial incentives for participation in federated identification systems, such as tax credits with criminal sanctions for their abuse?
- By using choke points – that is, requiring third parties such as Internet service providers, banks or the Internal Revenue Service to not transact business with the citizen unless they obtain and provide the mandated cyber identification?

Such regulation likely would require a massive expansion of the number of federal law enforcement agents or regulators. To date, the federal courts have struck down most state and local attempts at law enforcement or regulation of activities on the Internet as in violation of the dormant Commerce Clause of the United States Constitution. For example, state laws against child pornography, online gambling, spam, and using a false name online have all been declared unconstitutional by federal courts. Is such federal expansion desirable? Is it financially possible at present? Indeed, is government regulation of cyber identification enforceable, given that the U.S. government owns or controls only a minority (and a decreasing percentage of) devices and persons in cyberspace?

Within the general area of privacy arise issues of anonymity, attribution, and who should be empowered to strike that balance -- which some view as a balance between liberty and security. As noted above in section 1.1, the draft NS-TIC calls for the Federal Government to "create action plans to limit collection and transmission of information and to limit secondary uses, retention, and aggregation of data collected" (p.28).

According to Professor Snyder, Constitutional protections of privacy in cyber space are minimal. So, most privacy protections in a networked environment must come from statutes, not the Constitution. Thus, some current statutes criminalize data collections, retentions, disseminations

and aggregations prohibited by acts of Congress. Nevertheless, many things that can be done with and by data are not now prohibited by Congress.

Snyder reports that in the early 1970s when the enormous potential harm of computer misuse first became apparent, no state legislature had enacted a computer crimes statute. When prosecutors first began to bring charges for computer misuse, they naturally turned to physical crimes such as trespass, burglary, and theft. The fit of physical world crimes to the virtual world proved surprisingly poor. Our courts struggled with identifying a property interest that had been taken when, after the usual data theft, the owners still possessed the property. Several state legislatures tried different approaches until finally in 1986 Congress passed the Computer Fraud and Abuse Act.

That act makes it a crime to access a protected computer without authorization or exceeding authorization and thereby obtain information. Unfortunately, Congress did not define "exceeding authorization," and some courts soon concluded that any violation of an Internet service provider's user agreement constituted "exceeding authorization." Most user agreements are thousands of words long and contain nebulous prohibitions against uses that anyone else might find offensive. Moreover, we were told that this federal law would play a very limited role in our national system, because it only applies to "protected computers" defined as those in or involving interstate commerce. That may have been a meaningful limitation in 1986 before the World Wide Web, but today that definition includes every computer connected to the Internet and every cellular telephone.

Similarly, there was another tension about property rights reflected in another big legislative package in 1986 – the Electronic Communication Privacy Act. If you own a computer, then the data on it is yours, right? The constitute parts of the ECPA – including the Stored Communications Act – tried to balance that common sense notion of property with modern privacy expectations. The distinction was made between public and non-public providers. Thus, Google may not publish your emails to the entire world, but your employer or non-public provider such as an university may.

In general, these federal statutes made three distinctions between types of digital data, and these survive today.

1. Will the data be captured prospective or retrospectively?
2. Is it content or non-content data?
3. Does the owner of the hardware on which the data is stored offer service to the public, or not?

Based on these three attributes, the amount of legal process needed by either the government or a private entity like Google to access and share the data varies greatly – from nothing at all to so-called super warrants.

If the "action plans" of the NS-TIC to protect such data are to rely upon criminal law, then these statutes will need to be modified and expanded. In addition, criminal laws require an enforcement agency.

Dean Stanton believes that it is unlikely that the U.S. government could create a centralized law enforcement infrastructure with personnel to do the kind of work that needs to be done. He suggests encouraging the creation of commercial entities that would compete in a marketplace to create secure identities. This also would resonate with taxpayers by necessitating little additional tax money. Dean Elder notes that such a patchwork approach still would require centralized law enforcement oversight. We do not want marketers to connect the dots but we do want counterterrorism agencies to when monitoring terrorists. The dots are out there, but who gets to connect them is an important determination. Professor Rubin questions what such a government agency would look like and just what its role would be?

Snyder cautions that if law enforcement is to be given any role in protection and enforcement of trusted identities in cyberspace, then investigative procedural law will need massive restructuring at the same time. Law enforcement investigations in the cyber realm have proved to be very difficult, indeed. The very nature of Internet protocol communications divides them into packets of data that almost instantly cross jurisdictional boundaries. F.B.I. director Robert Mueller has decried the "patchwork of laws" his investigators face as making it nearly impossible to obtain digital evidence in a manner that will maintain its admissibility in our own courts. Howard A. Schmidt, the White House Cybersecurity Coordinator, has noted: “On the Internet there are no clues suggesting an international border has been crossed, yet sovereign rules still apply.” A workshop assembled by the American Bar Association concluded: “Thus in the criminal domain the single most significant question is one of extraterritoriality and engendering cooperation from international partners.” The Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency observed that current laws governing collection of electronic evidence may damage the nation’s cybersecurity, because “the sheer weight of legal complexity deters or delays investigations.” Although investigative procedural law may be beyond the scope of the Department of Commerce’s review, that body of law’s impact on enforcing rules that protect commerce underscores the need for government-wide review of cybersecurity policy.[7]

---

[7] Examples of these investigative law issues include:

- Should search warrants for digital evidence issued by United States courts be valid anywhere within the United States, regardless of the location of the issuing court or the nature of the matter investigated?
- Should the United States promote a unified, international procedure for investigating cybercrime and, if so, what should that procedure be and what foreign governments or international bodies should be encouraged to join? How should they be encouraged to join?
- Should the United States adopt procedures for remote execution of warrants authorizing the search and seizure of electronic data?
- Should Congress repeal Title 18, United States Code, Section 3109, which requires federal agents to “knock and announce” before the execution of search and seizure warrants, as it applies to searches conducted in cyberspace?
- How can procedures be streamlined so that both law enforcement and intelligence investigators can obtain the requisite judicial approvals for surveillance and searches in cyberspace at a speed consistent with the pace of events in cyberspace.
- How can the legal process for obtaining evidence internationally similarly be expedited?

Thus, argues Snyder, the U.S. experience demonstrates the limitations of law enforcement as a policy tool in cyber space. The regulation of a realm that knows no national borders cries out for a global solution, while the American public generally recognizes a social contract with -- and therefore the legitimacy of -- only those institutions created by its own Constitution. Law enforcement may be a necessary component of a National Strategy for Trusted Identities in Cyber Space, but it is certainly only a small part of the solution, he maintains.

Topic 3: Security, interoperability, trust, and trustworthiness

This section considers some of the systems engineering necessary to support the envisioned "Identity Ecosystem" of the NS-TIC. The term "ecosystem" is intended to connote a set of interacting components (hardware, software, protocols, certifications, and policies) whose combined behavior yields the intended properties of:

- security,
- interoperability,
- ease of use, and
- trustworthiness (confidence).

Professor Chin explains that two important points to remember about systems are:

1. It is impossible to optimize everything simultaneously, (e.g., one cannot build a car that simultaneously has the most horsepower while having the greatest fuel efficiency); and
2. Safety and security do not occur by themselves—they must be deliberately built in, (e.g., the Internet was originally a network for researchers who trusted each other; little or no network security was included in the original design).

As further explained below, security is sometimes at odds with interoperability and ease of use. For example, if banks desire the greatest security, the only means by which customers could withdraw funds from their accounts would be to appear in person at the bank branch that enrolled them as bank customers. This degree of security is in tension with ease of use and interoperability -- *e.g.,* allowing customers to use debit cards at ATMs and stores.

Details matter, so we will look in more detail at security, interoperability, trust, and trustworthiness.

3.1: Security

Professor Chin notes that security as a property typically has three components:

1. Confidentiality—who or what is allowed to see or know of a resource;
2. Integrity—who or what is allowed to draw from, modify, or change a resource; and
3. Availability—the quality or levels of service when accessing a resource.

Security *policies* describe what is acceptable or not regarding confidentiality, integrity, and availability. Describing a system as "secure" means that its behavior conforms to confidentiality, integrity, and availability policies. It is meaningless to talk about security without knowing precisely what is meant by the term.

Security policies may be *mandatory* or *discretionary*. Mandatory policies are policies that apply to everyone, without exception, all the time. For example, obeying traffic lights is a mandatory policy. Even first responders encountering red lights must take precautions. Discretionary policies are policies that are typically under the control of the subjects controlling resources. For example, social networking sites allow subscribers to specify who can see their information.

Clarity on all aspects of security policies is essential for *trust*. People lose trust in institutions or service providers if they feel or think that their notion of security is violated. For example, consider the continuing furor over Facebook's privacy policies and practices on status updates, personal information, and physical location.[8]

Loss of trust occurs because *expectations* are violated for reasons that include: misunderstood policies, inappropriate policies, failure to adhere to policies, failure to communicate changes in policies or practices, errors, fraud, attacks on the system, unintended consequences, and uncertainty. In Facebook's case, a change in their privacy practices, a new capability to track physical location, and uncertainty as to how to adequately audit who has access to what, have called into question Facebook's capability to handle personal information securely.

While the information contained in Facebook might be considered frivolous by some, it is not hard to see parallel perils in the handling of personal medical information, which is the continuing example used in the NS-TIC. From the standpoint of confidentiality, integrity, and availability, Professor Chin suggests consideration of the following scenarios.

- *Confidentiality:* Alice's health proxy is Bob. Alice and Bob are *not* related. Alice has specified that in the event she is unable to make her own decisions, then Bob is to be granted the authority to terminate life-sustaining procedures, if he deems the quality of Alice's life would be below Alice's minimum desires. What medical and financial information related to Alice's case is Bob able to see? Do the policies change if knowledge of Alice's information allows *Bo*b to infer the medical conditions of her children, siblings, or parents, that might be relevant to inherited diseases?
- *Integrity:* Suppose Bob is the only acceptable health proxy to Alice, but he is 12 time zones away and unable to be physically present. Assuming the validity and availability of the Identity Ecosystem postulated by the NS-TIC, is Bob—through his electronic identity—permitted to change Alice's medical records to include a "DNR—do not resuscitate" order?
- *Availability:* Suppose Bob is involved in a serious traffic accident while traveling 12 time zones away and is being attended to by physicians in a different country. The physicians deem Bob, who is unconscious, requires emergency surgery. The surgeons require

[8] Robert X. Cringely, *Can you trust Facebook Places?,* August 20, 2010, available at http://www.infoworld.com/d/adventures-in-it/can-you-trust-facebook-places-680 .

immediate access to Bob's medical records—how do they get *immediate* access 12 time zones away and bypass normal confidentiality restrictions in a timely fashion?

3.2: Interoperability and ease of use

Interoperability is defined by the NS-TIC as:

1. The capability of two or more networks, systems, devices, applications, or components to exchange and readily use information—securely, effectively, and with little or no inconvenience to the user, and
2. The ability of independent implementations of systems, devices, applications, or components to be used interchangeably. (p.33.)

The above definition is innocuous enough in appearance, but Professor Chin reports that it is both potentially complex and demanding of heroic engineering efforts by today's standards. This is *not* to say that today's standards of practice should not be improved -- they most certainly can and should be. Rather, the above observation is intended as a clear statement that to achieve reliable and trustworthy interoperability in the Identity Ecosystem will be complex and expensive.

To illustrate the difficulties that can arise with interoperability defined as the ability of applications and components to readily use information effectively, we need only recall the Mars Climate Orbiter. It was destroyed as a result of NASA interpreting data in metric units while Lockheed Martin interpreted the same data using English units.

While the loss of the Mars Climate Orbiter is a dramatic illustration of how seemingly innocuous and simple things such as numbers being interpreted as meters rather than feet can have catastrophic consequences, there are similar "simple things" lurking in the Identity Ecosystem that could cause problems. For example, take the interpretation of time. Most credentials or authorizations have an associated time or time limit. Time can be interpreted within the context of time zones (*e.g.*, GMT, GMT-5, EDST, etc.) or as the amount of time since a specified date and time (*e.g.*, 12 hours from issue date). The reference can be to a service provider's time, a client's time, or some third party's time. In the case of large-value commercial transactions, establishing whether a requested transfer falls within a valid period of authorization is critical. Establishing agreement on shared interpretations of information is important, necessary, and usually non-trivial.

The second aspect of interoperability -- the ability for independent implementations of the same systems, devices, applications, or components to be used interchangeably -- is potentially very expensive. The reason for much of the cost is the degree of precision and accuracy necessary to specify, test, and verify the behavior of systems, devices, applications, and components for all possible inputs and sequences of inputs. Specification, testing, and verification of this kind are usually reserved for only the most safety/security/life-critical applications and systems.

Professor Du argues that as a technical matter the "identity ecosystem" envisioned by the NS-TIC needs to be voluntary and not mandatory. He reports that he does not know how -- as a technical matter -- mandatory use in cyber space of trusted identities could be enforced.

Theoretically, we could verify trusted identities for all actions in cyber space, but the Internet "would be 100 times slower." In addition, mandatory use of strong identification will work only if all countries require it. Otherwise, our Internet Service Providers would go bankrupt as online servers migrate to places where mandatory participation is not required. That, he argues, is just competition, although it does not mean that every business cannot enforce a more restrictive policy. For example, a bank might institute its own policy that for transactions over $1,000,000, a customer must use trusted identification. If the customer wants to maintain anonymity, he simply may choose to not perform that transaction with that bank. Thus, from a technical standpoint, Professor Du supports the draft NS-TIC's proposed voluntary system.

3.3: Trust and trustworthiness

Professor Chin explains that in the context of information security, when you trust someone or something on a statement, their beliefs become your beliefs, or their authority governs your actions. For example, if Alice is trusted on matters related to money transfers, and if Alice says "transfer $1 million from account A to account B," then you do the transfer. Contrary to popular notions of trust, trust often is mandated, either by circumstances or by authority. People in organizations are told to whom they must listen and within whose scope of authority they reside.

Trust relationships are both explicit and implicit. In some organizations or for some transactions, trust or authority is transitive -- *i.e.*, trust or authority can be passed on or delegated. In other organizations or situations, trust or authority cannot be passed on or delegated. These properties must be documented and communicated clearly.

Trust is not the same as trustworthiness -- *i.e.*, being worthy of trust. Just because a system is trusted does not mean that it is trustworthy. Even when a person's or a system's commands/requests may not be ignored given their authority, the correctness of their commands/requests may be questionable unless they have been verified to be correct in all cases. This type of verification requires exactly the same kind and degree of specification, testing, and verification as required by interoperability. It is not simple, easy, or cheap.

To sustain trust in the Information Ecosystem, the *trustworthiness* of the ecosystem's components, networks, and devices must be established, monitored, and verified.

Professor Du believes that the NS-TIC is lacking an assessment of the identity system's trust computing base or "TCB." You cannot build security on top of air. In terms of identities, what do we trust short of implanting identifiers the moment a person is born? Something has to be trusted. It need not be technological, and, thus, trusted identities in cyberspace need more than a computer science solution. Du recommends considering the strategy as an engineering problem. First, we need people from a wide variety of disciplines to design the TCB. Only then can we determine how to build it. The requisite technology is available, he maintains.

Dr. Chin explains that ultimately the issues boil down to what will happen when there is a cyber request for some service: the provider must say yes or no. That will be determined not just by the technology or even by a properly authenticated identification. It will be determined by the policies designating who is trusted to make what statements and when. Policy is crucial to trust, even after the bits all line up. Who do we trust? Who is trusted and why is very situational, and thus one solution for trusted identities will not fit all.

In summary on Topic 3, Professor Chin believes that the technology envisioned by the draft NS-TIC is available, but that it will not achieve the goals stated on the first page of the strategy -- security, efficiency, ease-of-use, confidence, increased privacy, greater choice through interoperability, and increased innovation.

General Comments and Conclusions:

The majority of the panel finds the draft NS-TIC to be vague, difficult to read and difficult to understand. Complex as it is, the strategy addresses problems that are even more complex and difficult to resolve than the draft NS-TIC presents them to be. In addition, a system of trusted identities is but one part of an even larger and more complex national cybersecurity strategy that remains in only the beginning stages of development. The panel generally felt that the term "ecosystem" is a misnomer that inaccurately reflects how various actors and influences in cyberspace actually interact. There is no "silver bullet" solution to the problems of authentication and attribution in cyberspace – whether for commercial purposes or otherwise. Establishing, maintaining, and verifying trustworthiness are so expensive that priorities must be set. The solution lies in much hard work, research, difficult choices, and policy making of an uncommonly interdisciplinary character. Thus, the panel welcomes the inquiry by the Department of Commerce and recommends broader inquiries that include participants from across the federal government as well as the private sector, research institutions, and more.

WCS

- William C. Snyder

Appendix I

The draft National Strategy for Trusted Identities in Cyberspace (NS-TIC) offers four guiding principles, four goals and nine high-priority actions:

Principles:

Identity solutions will be:

1. Secure and Resilient
2. Interoperable
3. Privacy Enhancing and Voluntary for the Public
4. Cost-Effective and Easy To Use

Goals:

1. Develop a comprehensive Identity Ecosystem Framework.
2. Build and implement interoperable identity infrastructure aligned with the Identity Ecosystem Framework.
3. Enhance confidence and willingness to participate in the Identity Ecosystem.
4. Ensure the long-term success of the Identity Ecosystem.

High Priority Actions:

1. Designate a Federal Agency to Lead the Public/Private Sector Efforts Associated with Achieving the Goals of the Strategy
2. Develop a Shared, Comprehensive Public/Private Sector Implementation Plan
3. Accelerate the Expansion of Federal Services, Pilots, and Policies that Align with the Identity Ecosystem
4. Work Among the Public/Private Sectors to Implement Enhanced Privacy Protections
5. Coordinate the Development and Refinement of Risk Models and Interoperability Standards
6. Address the Liability Concerns of Service Providers and Individuals
7. Perform Outreach and Awareness Across all Stakeholders
8. Continue Collaborating in International Efforts
9. Identify Other Means to Drive Adoption of the Identity Ecosystem across the Nation

The entire text of the draft *National Strategy for Trusted Identities in Cyberspace: Creating Options for Enhanced Online Security and Privacy*, dated June 25, 2010, is available at http://www.dhs.gov/xlibrary/assets/ns_tic.pdf (last visited Sep. 17, 2010).

Appendix II

Biographies of the Panel Participants

William C. Banks
William C. Banks is a College of Law Board of Advisors Distinguished Professor at Syracuse University College of Law. He is a Professor of Public Administration at the Maxwell School of Citizenship and Public Affairs and he is also the Director of the Institute for National Security and Counterterrorism, which he founded in 2003. Professor Banks' current research interests include domestic and international terrorism, emergency powers, war powers, emergency preparedness and response, civil/military relations, and appropriations powers. Professor Banks has also co-written the leading text in the field. *National Security Law* was first published in 1990 and is now in its fourth edition. He and his co-authors published *Counterterrorism Law* in 2007 to help define the emerging field of counterterrorism law. Professor Banks received a bachelor's degree from the University of Nebraska and a master's degree and *juris doctor* from the University of Denver. Professor Banks joined the faculty of the Syracuse University College of Law in 1978. Since 1998, he also has been a Professor of Public Administration in SU's Maxwell School of Citizenship and Public Affairs. He was named the Laura J. and L. Douglas Meredith Professor for Teaching Excellence in 1998. He also served as Special Counsel to the United States Judiciary Committee in 1994. Professor Banks worked with the committee on the confirmation hearings for Supreme Court nominee Stephen G. Breyer. He currently serves as a member of the International Institute for Counter-Terrorism's International Advisory Council for the Perpetual Peace Project sponsored by the Slought Foundation, and on the Advisory Board for InfraGard.

Glenn Benson
Mr. Glenn Benson is the security architect of JP-Morgan Chase Treasury Services. Dr. Benson’s responsibilities include all aspects of security architecture covering hundreds of applications that cumulatively process more than USD 3 trillion daily. Dr. Benson received his PhD from Georgia Institute of Technology, and has worked throughout his entire career in the information security industry. Dr. Benson has five patents, and additional patent applications.

Shiu-Kai Chin
Professor Shiu-Kai Chin is Meredith Professor at the L.C. Smith College of Engineering and Computer Science (LCS) at Syracuse University. Professor Chin's research applies mathematical logic to the engineering of trustworthy systems. Prior to joining Syracuse University in 1986, Professor Chin was a senior engineer and program manager at General Electric for 11 years. Chin received his doctorate in computer engineering at Syracuse University in 1986. In addition to being an instructor in the Air Force Research Laboratory's Advanced Course in Engineering Cyber Security Boot Camp, Chin has served as a program director of Computer Engineering at the L.C. Smith College of Engineering and Computer Science until 2006. From 2006 to 2008 he was the interim dean of LCS. Professor Chin received the Crouse Hinds Award for Excellence in Education from LCS in 1994. In 1997, he was appointed Laura J. and L. Douglas Meredith Professor for Teaching Excellence, Syracuse University's highest teaching award. In 2002, he received the Chancellor's Citation for Outstanding Contributions to the University's Academic Programs.

Sean Croston
Sean Croston is Vice President and Senior Product Manager, JP-Morgan Chase Bank. Mr. Croston is globally responsible for the security arrangements relating to JP-Morgan's online banking platforms, Host to Host, Workstations and JP-Morgan ACCESS. Prior to this, Mr. Croston was co-founder and managing director at FirmLink Networks. Mr. Croston has also served as Director of Financial Markets at Savvis. Mr. Croston is an alumnus of Bentley University, Class of 1990.

Lisa A. Dolak
An Angela S. Cooney Professor of Law, Professor Dolak's research interests include issues at the intersections of patent law and judicial procedure, patent law and the media, and patent law and legal ethics. Her current research projects focus on media coverage of the U.S. patent system, the effects of the evolving inequitable conduct doctrine on the practice of patent law, and a reconsidered theory of subject matter conflicts. She teaches courses on patent law, Internet law, and practice and procedure in the federal courts. She is a registered patent attorney and a *summa cum laude* graduate of Syracuse University College of Law. Professor Dolak also serves as Associate Director at the Center on Property, Citizenship, and Social Entrepreneurism and as an Associate Director at the Institute for the Study of the Judiciary, Politics and the Media.

Kevin Du
Wenliang (Kevin) Du is an Associate Professor at Syracuse University's Department of Electrical Engineering and Computer Science, specializing in the areas of computer, information, and network security. His research focuses on the areas of privacy-preserving data mining, web security and privacy, and computer security education. Professor Du received his Doctorate in Computer Science from Purdue University, 2001.

Randy Elder
Randy Elder is the Senior Associate Dean at the Whitman School of Management at Syracuse University. Dean Elder's research focuses on audit quality, governmental auditing, and auditor decision-making. He received his doctorate in accounting from Michigan State University.

David M. Rubin
David M. Rubin was Dean of the S.I. Newhouse School of Public Communications at Syracuse University from July 1990 to June 2008. During his tenure, the School founded the Bleier Center for Television and Popular Culture; the Healthy Campus Initiative (to study which health communications messages have resonance with a young audience), and the Institute for the Study of the Judiciary, Politics and the Media. Additionally, Dean Rubin has twice served as a Pulitzer Prize juror. He headed the Task Force on the Public's Right to Know for the Presidential Commission on the Accident at Three Mile Island Nuclear Power Plant, producing a detailed report on the flow of information during that incident. He has written extensively about media law and ethics, and about the business of classical music. Dean Rubin was on the faculty at NYU from 1971-1990 and was recruited from NYU to the position of Dean at Syracuse. He holds a B.A. from Columbia College in New York City, and M.A. and Ph.D. degrees from Stanford.

William Snyder
William C. Snyder is a Visiting Assistant Professor at Syracuse University College of Law where he has taught *Federal Criminal Law*, *Computer Crimes*, *Counter-Terrorism and the Law*, *Prosecuting Terrorists in Article III Courts*, *Cyber Security Law & Policy*, *Federal Courts* and *Evidence*. In addition, he assists at the Institute for National Security and Counterterrorism, a joint venture of Syracuse University's College of Law and its Maxwell School of Citizenship and Public Affairs. Professor Snyder was the 2004-2005 Fellow in Government Law and Policy at the Albany Law School's Government Law Center. A career federal prosecutor prior to joining the Government Law Center, Professor Snyder served over 13 years as an Assistant United States Attorney (AUSA) in the Western District of Pennsylvania and the District of Columbia. Prior to receiving his law degree, Professor Snyder served as an Assistant to the Attorney General of the United States and was Deputy Administrative Assistant to Pennsylvania Governor Dick Thornburgh. Professor Snyder received his Bachelor of Arts degree *cum laude* in political science with a concentration in international relations from Yale College of Yale University. He received his *Juris Doctor* degree *magna cum laude* from Cornell Law School where he served on the *Cornell Law Review* and was elected to the Order of the Coif.

Jeffrey M. Stanton
Jeffrey Stanton is the Associate Dean for Research and Doctoral Studies in the School of Information Studies at Syracuse University. Professor Stanton received his Doctorate from the University of Connecticut in 1997. Dr. Stanton's research focuses on organizational behavior and technology, with his most recent projects examining how behavior affects information security and privacy in organizations. He is the author with Dr. Kathryn Stam of the book, *The Visible Employee: Using Workplace Monitoring and Surveillance to Protect Information Assets – Without Compromising Employee Privacy or Trust.*