

On OIX and NSTIC

by Don Thibea

Overview

This document provides a high-level survey of the relationship of the National Strategy for Trusted Identities in Cyberspace (NSTIC) and OIX. Through an explanation of the Public-Private Partnership (PPP) rulemaking process, the document will identify the programs and actions called for in NSTIC and demonstrate how OIX's programs and tools will support the strategy's development.

This material is intended to explore the complimentary roles and relationship of the US federal government and the commercial sector in the quickly evolving data/identity markets. After a brief review of NSTIC, this material explores the policy leadership issues from a policy-making *process* perspective. The policy process is presented in the form of an empirical analysis of the five stages of rulemaking in the public/private context, borrowed from policy sciences literature.¹ The five stages of rulemaking are: *agenda setting* (discussion of issues), *problem identification* (focusing on relevant variables), *decision* (define future action items), *implementation* (focus on deployment), and *evaluation* (assessment of implementation and new *agenda setting* cycle). This material avoids the role of individual stakeholders, but only for purposes of this discussion, and not to diminish the critical importance of that stakeholder group. The substance will maintain a particular emphasis on the interests and rights of individuals.

OIX began modestly in response to a call from the US CIO. As the data/identity markets have quickly evolved, new and expanded roles for OIX have suggested themselves, each with benefits for different stakeholder groups. Because at least one agency of the US government (the GSA), has already recognized OIX as fulfilling a market leadership role (through its TFPAP process), and because OIX organization and operation is intended to provide neutral, broad data/identity market support, OIX is a natural candidate for consideration toward helping to coordinate policy and rules development at the commercial/governmental interface.

Conclusion

The materials conclude that, even though the OIX programs and tools were originally put in place in response to the call by the GSA to address US government credentialing and identity system needs, those same OIX programs and tools (and the new markets that they support) can be of value to all data/identity system stakeholders, not just to the U.S. in its role as a “relying party” as emphasized in GSA’s FICAM program. Not only can OIX help to “unpack” data/identity value elements and structured benefits to all stakeholders, but OIX is in a good position to help “coordinate” the identification and preparation of stakeholder rules that balance stakeholder interests.

NSTIC

¹ In particular, the article “Self-regulation as policy process: The multiple and criss-crossing stages of private rule-making” by Tony Porter & Karsten Ronit (Policy Sciences, 2006)(Ronit 2006), is relied upon for the basic structure reflected here. That article surveyed dozens of hybrid public/private rule making settings in various countries to derive the five stages reflected here.

NSTIC is a request for assistance. Just as the US government doesn't manufacture its own trucks, airplanes and guns, it also will not produce its own identity system infrastructure. NSTIC provides a set of guiding principles,² and provides a vision statement that "Individuals and organizations utilize secure, efficient, easy to use and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice and innovation." NSTIC introduces the concept of an "identity ecosystem" can be variously called a commercial market, a social community or a political governance structure depending on the context in which the data/identity system is being applied.

The GSA FICAM was one way that the US asked for help, but was in the narrower context of the government's data/identity system credentialing needs as a relying party. NSTIC is a broader call for coordination and assistance, with greater deference to private sector policy setting that is necessary for the broader program anticipated in the document. The "identity ecosystem" called for by NSTIC is at the core of current and future data/identity systems that are operated by OIX members.

NSTIC provides four goals³ and establishes nine high priority actions to pursue those goals. The rulemaking process at the center of PPPs suggests that NSTIC-based initiatives will likely proceed through five stages.

I. Stage 1 - Agenda Setting

Agenda setting is the first stage where different groups raise issues in related areas and where different groups identify and explore conflicts with other groups. Successful agenda setting for data/identity rules will be a hybrid of public and private processes. For maximum efficiency and to enable greatest stakeholder participation, the different rulemaking processes should be loosely coupled into separate but coordinated efforts.

A substantial part of the current data/identity discussion is locked in the agenda setting process. Since NSTIC has a strong public component, success will go to the market participants that can help provide solutions to public concerns. But since those concerns are ill defined, so the exercise is as much about expectation setting as anything else.

The advantage of a PPP at this stage is that it offers greater flexibility and informality in rulemaking than public law. In a PPP situation, there can be agreed-upon aspects of system legal development that can be developed in either the private or the public sphere to match the context giving the process flexibility.

That OIX membership does not include all potential IDP players is not a problem; greater normalization of any sub-part of the market through the development and adoption of standard rules will have potential benefits to all stakeholders. The work of OIX, as stated

² Those principles are: that identity solutions will be secure and resilient; that they will be interoperable; that they will be privacy enhancing and voluntary for the public; and will be cost effective and easy to use.

³ The four goals are: 1. Develop a comprehensive identity ecosystem framework, 2. Build and implement interoperable identity infrastructure aligned with the common identity ecosystem framework, 3. Enhance confidence and willingness to participate in the identity ecosystem, and 4. Ensure the long term success of the identity ecosystem.

in its purposes, is to benefit and improve conditions in the industry generally. If any businesses are interested in participating in the future they are free to join OIX.

II. Stage 2 – Problem Identification

Problem identification is the stage where issues raised during “agenda setting” are narrowed to those that lend themselves to the crafting of rules and solutions for the stage 3 Decision. The second stage exercise of “problem identification” can be thought of as the capturing and specification of issues/problems “signal” from the “noise” of agenda setting. In other words, the improvement of the “signal to noise” ratio does not require that any stakeholder agenda items be ignored, only that they be coordinated with other issues into problem identification “slots.”

The OIX working groups structure was designed to allow the easy separation of issues/discussions into groups and subgroups as needed to foster efficient, transparent and participatory development. Each OIX working group is separate, can determine its own IPR and governance policy, and is able to follow its own work plan at its own pace.

Traditional rulemaking will likely result in the perpetuation of jurisdictional silos, raising compliance costs for data/identity service providers and other stakeholders across multiple jurisdictions. However, a PPP can leverage large firm reach to allow policy transfer across jurisdictions, especially with regard to data/identity services which play an increasingly important role in many industries that these bridges are available. Comprehensive trust frameworks are the cheapest to build, since more parties promises to perform duties in accordance with a given standard of care are available as the “currency” to pay to other participants.

III. Stage 3 - Decision making

Decision making involves the selection of stage 2 “problems” to address and the making of decisions and new rules of how to deal with them. PPP begins to show its truly unique value at this stage, as it elevates all participants to the role of virtual “members of the legislature,” providing access to mechanisms of rules creation to those parties that are affected by the rules.

The OIX working group structure makes it easier to compare progress across and among initiatives. The OIX working group community provides the benefit of seeing how others handle various issues. One area in which NSTIC seeks to guide the decision making process is through its promotion of FIPPs-based legislation. The Department of Commerce Green Paper suggests that an updated set of FIPPs is a necessary starting point for decision making, and a PPP arrangement would allow a variety of perspectives and approaches to the question of FIPPs standardization.

IV. Stage 4 – Implementation

During stage 4, implementation, the focus shifts from rulemaking system to deploying systems, which involves issues of applying incentives and penalties to coax participation.

PPPs enable standardization of legal rules to help support standardization of technology tools. If private parties are involved in rule setting, they can better configure new rules to integrate them in more easily, thereby helping to defray the educational and other deployment costs that plague government-only rulemaking. PPP can encourage membership (particularly of reluctant larger firms), by encouraging other entities to adopt PPP-derived rules. If such peer pressure doesn't work, industry can always fall back on the capacity and expertise of public sector enforcement capabilities.

V. Stage V - Evaluation

During the evaluation stage there is assessment and reporting of the activities engaged in during implementation. Evaluation involves both the review of prior actions and the initiation of corrective actions. Governmental rulemaking in the form of legislation or regulation does not typically anticipate being subject to dynamic alteration based on effectiveness reviews. In addition, private evaluation processes are atypical simply because they are infrequently bothered with during process planning. Where PPP processes are engaged in, the evaluation steps can be more formalized, making possible better evaluation, and improved process improvement, with the anticipation that private involvement makes corrective changes easier.

- **VI. Other Considerations**

- Relying parties include several developed industries of long standing, that are well organized into consortia. Like all groups, relying parties will want to push increased responsibility onto other parties in the system, including the identity providers. That is one of the observations made about current FICAM requirements; i.e., that they are not commercially viable because they put too much of the resource responsibility on identity providers. The system cannot be built at scale without balance.
- The US government is involved in the process of seeking reform in the regulation of the financial and healthcare areas. These are two large relying party groups that would be subject to RP-BP based duties in a data/identity ecosystem. A PPP can help coordinate such reform initiatives.
- For current purposes, it is sufficient to observe that, whatever the particular market involved, consumers and other market participants are not enjoying all of the choices that they might in a mature, expanded market. This suggests that the market is not fully functioning, with potential negative effects on participants. For instance, is consumer “consent” to a social network terms of service a valid way to test consent if the consumer has only one choice of service? Are commercial market participants able to effectively compete if they are bound to the terms of a single market player? It is not necessary to explore the details of legal definitions of markets to observe that the absence of choice has the potential to produce harm. The issue is complicated by the fact that many of the measures of “success” in the data/identity markets are tied to the network effect that arises from having broad system adoption.
- It is possible to continuously improve market conditions to the benefit of all participants if the market itself can be brought into service in the effort. In other words, to move the market, it is necessary to move (business and individual) consumer expectations.
- This is a unique setting, since the US government is also looking to the commercial markets to provide it with access to effective data/identity solutions. That means that a lack of consumer choice causes a lack of US government choice (since the US government is itself a “consumer” of the services offered in the market). This can become a cause of more than just inconvenience for a government.
- The current PPP discussion might therefore offer a rare opportunity when government will support organized effort of market participants to help create standards that can affect market expectations and thereby help to continuously re-set market structure.
- OIX is intended to provide members with an opportunity to participate in the market structuring exercise, and to support the creation and broad publication of tools and programs to enable stakeholders to participate, leading to a broadly open and competitive market that encourages a “race to the top.”.

- A government-supported PPP has even greater potential for moving markets to encourage broad adoption of standards around data/identity best practices than do individual firms working in isolation. Also, government action may be more direct, i.e., if the market approach fails to address the free rider and non-member problem, and consumers and market participants experience a lack of open, competitive markets, the government can consider action through legislation or regulation as needed to regularize and normalize the markets.
- A PPP will have a much better chance of helping to focus that legislation than individual companies can.
 - RPBP
 - Data-related Systemic Risk Management benefits
 - Data-related Systemic Liability Management benefits
 - Cost effective compliance (e.g., for privacy and security requirements)
 - Consumer Product Market Development (maturation and refinement of products)
 - Mitigated government regulation
 - Safe harbor legislation
 - Investment, tax and other incentives
 - International aspects:
 - Decreased international legal compliance costs
 - Increased geographic market penetration (global PPP can do all of the preceding across jurisdictions)
 - Increased leveraged market growth across jurisdictions
- Getting a chance to comment on government legislation, regulation and policies is good. Getting a chance to draft policy (and to let others comment on your draft) is better.
- IDPs can act now to increase their organization and cohesion, and to take advantage of the NSTIC opportunity, so that when liability issues arise, they can be addressed structurally (through the control of the rules effort), not just through individual negotiations of indemnity provisions and other secondary strategies.
- **Q: Does engagement in PPP offer cost savings opportunities?**
- A: Yes. The uniform rules resulting from a PPP effort will result in cost savings by enabling reduced compliance costs savings and dispute resolution cost savings
- Arbitration “lifts” disputes out of those settings and allows it to be pursued at a more normalized, predictable way, without needing to know the details of 200 countries’ laws to run an international system. This results in very significant cost savings.

- This leaves open the question of how online micro disputes can best be resolved in future data/identity systems. Dispute resolution in that context will require a standardized international system that can “lift” the disputes out of the tangle of local law where possible and appropriate for the preservation of system user rights. Future systems may involve automated processes and/or “arbitration-lite” type systems that take advantage of online and social network functionality to enable deployment at greater scale.
- This type of international system to save compliance and dispute costs cannot be achieved by a single company, and it is not instrumented by a single country.
- The standard OIX trust triangle, with each party having mutually dependent rights and duties, trust on the cheap
- Draft NSTIC calls for FIPPs legislation. OIX produced the “FIPPs Analysis Tool” and has taken on the question of how FIPPs might be operationalized at the lowest cost and for the maximum stakeholder benefit.
- The accounting profession had a long tradition of self regulation (being left alone by government) that it lost in the wake of the Enron scandal.
- There is precedent for government action where the accumulation of market power, even by innocent and fair practices, still led to a situation where the ill effects of a lack of competition were felt by other consumers and other market participants.
- OIX was designed to provide equal access to market development resources to combat this perception and to assure open access. For example, the open listing service requirements, the open access to OIX Trust Framework development tools, the limitation on confidentiality of contributions to OIX and the open format working groups structure are intended to provide equal access to OIX programs to any parties that are interested in engaging in Trust Framework development and deployment from any trust community reflecting the interests of any one or more stakeholder groups.
- First, the advisory board is intended to establish a relationship with recognized experts in related fields to help provide multiple perspectives on the work of developing and then maintaining a market in which Trust Frameworks play a central role.
- Second, by maintaining the OIX knowledge center (formerly the risk wiki), current market relevant information and product development ideas are brought into a central resource to help inform individual stakeholder product development and purchase decisions.

- Third, the OIX working group community brings a great deal of development activity under the general auspices of OIX, even if the working groups have greatly different governance and IPR structures.

- **Q: What are the factors that a PPP needs to survive?**

- A: Efficiency, legitimacy, standards and transparency
- OIX has been structured for maximum transparency in organization and operations. OIX offers efficiency in the form of a highly developed Trust Framework development tool set. Finally, legitimacy is established by nature of the membership of OIX, its links to international data/identity initiatives, and its demonstrated ability to generate programs and tools to enable Trust Frameworks and in supporting the maturation of the data/identity markets..
- The “continuum” of forms of regulation range from laissez-faire to pure government regulation, with (in order of increasing governmental involvement and influence after laissez faire (aka “none)), pure self-regulation, co-opted self regulation, negotiated self regulation, mandated self regulation (See Ronit (2006). These may vary on different sub-issues and at different stages of rules development.
- The promotion of FIPPs legislation in the NSTIC is an example of “mandated self-regulation.” That is because if it passes, it will establish a set of *de facto* standards, but it still needs implementation through rules derived from “self regulation.”
- The GSA FICAM effort is currently has become an example of “negotiated self regulation (since the GSA made an “offer” at higher LOAs for which the commercial sector will likely make a “counteroffer.”) The Commerce Department “Green Paper” can be seen as promoting an example of “self regulation”

- **Q: What about a self assessment regime without a PPP setting standards?**

- A: Online data/identity systems rely on trust. Standard rules enable reliability and predictability that are the foundation of trust. Third party assessment against standard rules enhances that trust. The absence of either standard rules or third party assessment makes it more difficult to establish trust, raising costs across systems.
- A: OIX is designed to help absorb the strain associated with providing an interface between future internet scale data/identity infrastructure and current national and industry-constrained data/identity systems. That “strain” is partially absorbed through the OIX working group program, that divides governance between “market administration decision making” (which resides in the OIX board), and “Trust

Framework development decision making” (which resides in the working group participants). Cp NYSE

- Thus, although OIX helps to enable the establishment of market-based standards, the ultimate decision authority on Trust Framework standards remains within the Trust Communities that draft the Trust Frameworks (only the decisions on market operations rest with OIX). The nature of the Trust Frameworks composed by various trust communities ultimately defines the data/identity market characteristics for each of them. OIX programs and tools merely promote their normalization and interoperability.
- OIX working groups have the ability to draft their own governance documents, IP policies, etc. They can invite participation of all stakeholder groups, and they can craft Trust Framework materials of any scope desired (including those intended for national domestic application such as the US Trust Ecosystem). By becoming part of the OIX WG community, there is greater access to OIX tools, the advisory board, and a close relationship to the market itself. This would allow transparency, open participation, and a host of other benefits to both parties, but not “slow down” or make “U.S.-centric” the overall work of OIX.