NSTIC's Effect on Privacy

The Need to Balance Identity and Privacy-Protection with Market Forces in the National Strategy for Trusted Identities in Cyberspace

April 15, 2011

By Identity Finder, LLC: Aaron Titus, Todd Feinman, and David Goldman

The National Strategy for Trusted Identities in Cyberspace (NSTIC) is a government-coordinated initiative to create a national private-sector digital identity system. This report identifies technology-independent privacy and security vulnerabilities that NSTIC policy must address through technology, policy and regulation.

If implemented properly, NSTIC could improve privacy. As an aspirational document, NSTIC makes privacy a core principle but stops short of recommending regulation to ensure privacy. Without a regulation to implement NSTIC, powerful identity credentials will, if lost or stolen, enable hyper-identity theft. Market forces will likely 1) create a false sense of control, privacy, and security among users; 2) enable new ways to covertly collect users' personal information; and 3) create new markets in which to commoditize human identity.

identityfinder

Highlights of this Report

Identity Finder (www.identityfinder.com) commends the White House and Department of Commerce for establishing a framework to improve the assurance levels of online transactions. More efficient transactions should lower costs for consumers and enable new services not currently possible.

If implemented within a proper regulatory framework, an ideal NSTIC Identity Ecosystem could establish:

- High levels of identity assurance online, increasing trust between Users and service providers.
- More secure online transactions.
- Innovation and new services.
- Improved privacy and anonymity.
- Increased convenience for Users and savings for service providers.

To successfully implement its visions of privacy, security, and secure identities, the NSTIC implementation must call for Federal regulation which will:

- Hold all Identity Ecosystem Participants to legal and technical standards which implement Fair Information Practice Principles (FIPPs) and baseline privacy and security protocols.
- Create incentives for businesses to not commoditize human identity.
- Compensate for an individual's unequal bargaining power when establishing privacy and data usage policies.
- Subject Identity Providers to similar requirements to the Fair Credit Reporting Act.
- Train individuals on how to properly safeguard their Identity Medium to avoid identity theft.
- Ensure that consumers and advocates have a meaningful voice in the development of NSTIC policy.

Without regulatory policy, procedural safeguards and mandatory technology standards, NSTIC will fall short of its aspirations and may do more harm than good, creating the following results:

- New ways to covertly collect personal information, and new markets to commoditize Users' identities.
- New, powerful credentials that will subject individuals to new risks of identity theft.
- Identity Ecosystem Participants may not need to comply with industry baseline security or privacy protocols.
- An enhanced Identity "Marketplace" which enables Participants to profit from the sale of human identities.
- The Identity Ecosystem "Marketplace" would continue to be opaque to users, and may create a false sense of control, privacy, and security among Users who are unaware that their identities are subject to sale without their knowledge.
- A User who opts out of the Ecosystem may also inadvertently lose privacy protections.
- New, powerful NSTIC identity credentials will enable the same functionality as an Internet "Power of Attorney," without the procedural safeguards offline Powers of Attorney provide.

Given the risks NSTIC pose to privacy, the Department of Commerce, NIST, and the White House should be more transparent about the unsolved privacy and security hurdles associated with deploying a nation-wide framework of federated identity systems.

Identity Finder had hoped that the issue of regulation would have been addressed in the April 15, 2011 NSTIC document. We now hope that policy-makers will make the vulnerabilities identified in this report the subject of future development, discussion, and regulation. Identity Finder stands ready to contribute to that process.

Executive Summary

Today, identities are bought and sold in a clandestine multi-billion dollar industry. Breaches of personal information occur on a daily basis,[1] and Identity Theft remains a growing crime in America with over 9 million victims each year.[2] Social Security Numbers, dates of birth, and mothers' maiden names continue to be stored and used insecurely by organizations in every industry.

The National Strategy for Trusted Identities in Cyberspace (NSTIC) is a Federal Government initiative to encourage the private sector to develop a national framework of independent and interoperable federated identity systems. Together, these interoperable systems and their participants are called the "Identity Ecosystem." Each identity system within the Ecosystem would be privately owned and operated, and utilize a range of technologies. The federated identities such systems support are portable across multiple systems, meaning an individual could authenticate to several online resources using a single credential or Identity Medium.

U.S. citizens were given a social security card, and it took us decades to realize that we should not carry them around in our wallets. Now citizens are being given a more powerful form of identification, and being told it is okay to carry it on our phones, tablets, laptops, and computers.

U.S. citizens were given a social security card, and it took us decades to realize that we should not carry them around in our wallets. Now citizens are being given a more powerful form of identification, and being told it is okay to carry it on our phones, tablets, laptops, and computers. We must anticipate the risks that will inevitably follow.

The Department of Commerce, which leads the government's efforts in developing NSTIC, has publicly called for privacy legislation independent of NSTIC, and is working on security legislation with the Obama Administration. While NSTIC acknowledges the need for rules to minimize abuse of federated identity technology tools, it stops short of calling for particular policies, laws, or regulation mandating privacy or security. The strategy attempts to stimulate private industry to build and self-regulate the Identity Ecosystem.

If implemented correctly, a national framework of interoperable federated identity systems could have a net positive effect on privacy, as organizations replace insecure methods of identification (such as the Social Security Number) with more secure identifiers and authentication methods. NSTIC represents an opportunity to improve users' privacy and move beyond Social Security Numbers (SSNs), Dates of Birth, and Mothers' Maiden Names as a method of authenticating identities. Identity Finder supports NSTIC to the extent that it can decrease the trade of personally identifiable information, help individuals secure private data, and regain control over their identities. Existing technology, if implemented properly, could secure online transactions, improve identity authentication, and decrease transactional costs, while improving privacy and ensuring real online anonymity.

Unfortunately, the mere existence of a beneficial technology does not make its use inevitable. Just as a hammer may be used for construction as well as demolition, federated identity technology may also be implemented in a manner that destroys privacy, eviscerates anonymity, and increases the clandestine market for personal information.

This report concludes that the exchange of data and money through a typical federated identity transaction creates multiple market incentives to use technology that will increase profits at the expense of privacy. The unregulated Identity Ecosystem envisioned by NSTIC will open new markets for buying and selling personal information and, absent policy to the contrary, would create new security risk vectors for individuals who participate in the Identity Ecosystem.

To counteract these market forces, NSTIC policy should contain unambiguous and mandatory restrictions on how NSTIC participants may use

[1] The Open Security Foundation maintains a fairly comprehensive database of reported breaches called the Data Loss Database: http://datalossdb.org/

[2] *See FTC Identity Theft Facts*: http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html

sensitive personal information based upon well-accepted Fair Information Practice Principles (FIPPs). NSTIC elevates privacy as an indispensible tenant of the Identity Ecosystem, and recognizes the need to place limits on secondary use of personal information, but stops short of recommending regulation to enforce those policies. Because the final draft of NSTIC[3] does not explicitly call for a regulatory framework, we hope that forthcoming NSTIC implementation documents will address this vital issue.

We fear that without a near Herculean effort in future implementation plans, NSTIC policy will have a net negative effect on privacy, driving privacy practices to lower levels than they otherwise would be. We hope that the Identity Community, which has spent years developing privacy-enhancing protocols, will demand that NSTIC require those best practices as a matter of policy. We encourage entrepreneurs to develop new business models that do not monetize human identity. And we urge federal officials at the Department of Commerce to acknowledge the tremendous hurdles to privacy and security which remain unsolved, before they make public assurances that NSTIC will inevitably improve privacy.

[3] A link to the final version of the *National Strategy for Trusted Identities in Cyberspace* (April 15, 2011) may be found at http://www.nist.gov/nistic

Table of Contents

Introduction to NSTIC

Brief History

The National Strategy for Trusted Identities in Cyberspace (NSTIC, pronounced 'N-Stick') is a White House[4] initiative to encourage large-scale private development and adoption of interoperable federated identity systems. The initiative is led by the Department of Commerce and the National Institute of Standards Technology (NIST),[5] with close coordination among the Departments of Health and Human Services, Homeland Security, Treasury, General Services Administration, and Veterans Affairs.

NSTIC is a vision and strategy to encourage the private sector to develop multiple technologies for a large-scale NSTIC "Identity Ecosystem." Prudent implementation of the NSTIC Identity Ecosystem could bring major benefits to consumers, citizens, the public discourse, and online commerce.

NSTIC's roots date to Presidential Decision Directive 63 (PDD-63), signed in May 1998. The policy was updated in 2003 with *The National Strategy to Secure Cyberspace*. A draft of the NSTIC Strategy Document was released on June 25, 2010[6] and the final draft of the NSTIC Strategy Document was released on April 15, 2011.[7]

Need for Authenticated Transactions

Although advertisers continue to develop new ways[8] to identitfy users online, the Internet lacks what identity professional Kaliya Hamlin calls a "trust" or "identity layer."[9] In other words, without a reliable method for verifying identity online, "on the Internet, nobody knows you're a dog."[10]

As explained by Kaliya Hamlin, there are five fundamental types of identity verification:

- **Anonymity**: The complete non-knowledge of an actor's identity.
- **Pseudonymity**: When an actor uses a pseudonym in place of his/her real name.
- **Self-Asserted Identity**: When an actor asserts his/her identity, without third-party verification.
- **Verified Identity**: When a trusted third party confirms an actor's identity.
- **Verified Anonymity**: When a third party verifies one or more attributes about an actor, where those attributes are insufficient to be personally identifying.

While anonymous, pseudonymous, and self-asserted identification may be sufficient for blogging and web surfing, they may be insufficient when interacting with banks, healthcare providers, or buying a house. Without a reliable method to verify identities, service providers incur uncertainty and cost. The problem of untrusted identities is illustrated in **Figure 1**.

Figure 1: Untrusted Identity

The Federated Identity solution to untrusted identities online is to introduce a trusted third party who verifies a User's identity, as illustrated in **Figure 2**:

[4] *The National Strategy for Trusted Identities in Cyberspace*, Howard A. Schmidt, June 25, 2010 http://www.whitehouse.gov/blog/2010/06/25/national-strategy-trusted-identities-cyberspace (Accessed March 28, 2011).

[5] National Institute of Standards and Technology, *National Strategy on Trusted Identities in Cyberspace*, http://www.nist.gov/nstic/ (Accessed March 28, 2011).

[6] *National Strategy for Trusted Identities in Cyberspace*, June 25, 2010, http://www.dhs.gov/xlibrary/assets/ns_tic.pdf (Accessed March 28, 2011).

[7] *See* http://www.nist.gov/nstic for a link to the Strategy

[8] See, e.g., the Electronic Frontier Foundation's browser fingerprint demonstration project, *Panopticlick* at http://panopticlick.eff.org/ (Accessed March 28, 2011)

[9] Kaliya Hamilton, *Thoughts on the National Strategy for Trusted Identities in Cyberspace*, June 25, 2010, http://www.identitywoman.net/thoughts-on-the-national-strategy-for-trusted-identities-in-cyberspace (Accessed March 28, 2011)

[10] For more background information about Peter Steiner's famous *The New Yorker* cartoon, see, http://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog (Accessed March 28, 2011)

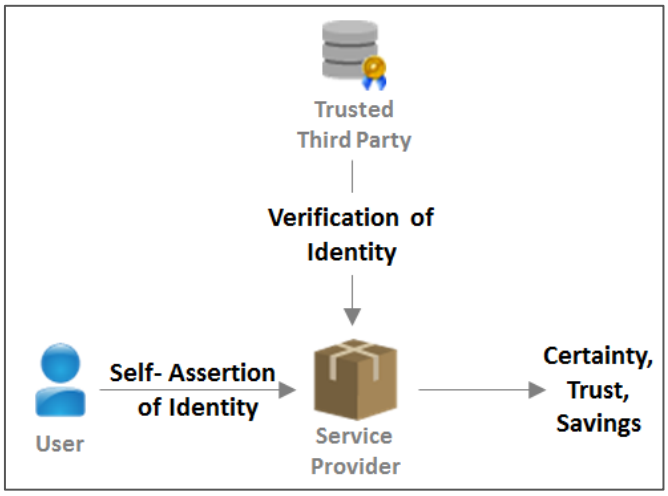

Figure 2: Establishing a Trusted Identity

Introducing a trusted third party in online transactions could have the following benefits to establishing verified identities online:

1. High levels of identity assurance online, thus increasing trust between Users and service providers
2. More secure online transactions
3. Innovation and new services
4. Improved Privacy
5. Increased efficiency and convenience for Users and service providers

Identity Ecosystem Marketplace

NSTIC envisions a secure "Identity Ecosystem Framework," or "the overarching set of interoperability standards, risk models, privacy and liability policies, requirements and accountability mechanisms that structure the Identity Ecosystem."[11] While the Identity Ecosystem will provide value to any participant which needs to verify a User's identity, the Ecosystem will provide the most value to businesses which commoditize human identity. We identify the resulting market as the "Identity Ecosystem Marketplace." An Identity Marketplace already exists, and has been admirably illustrated by Luma Partners, LLC[12] and Improve Digital.[13]

Possible Implications of NSTIC on Privacy

The International Association of Privacy Professionals (IAPP) hosted an "NSTIC Listening Session" on March 10, 2011. The panel discussion included Helen Foster of the Department of Homeland Security's Privacy Office; Jeremy Grant, Senior Executive Advisor at NIST; Naomi Lefkovitz, White House National Security Staff; Ari Schwartz of NIST, formerly of the Center for Democracy and Technology; and moderated by Jules Polonetsky, Co-Chairman and Director of the Future of Privacy Forum.

During the meeting, Identity Finder's Aaron Titus, an author of this report, raised several concerns about NSTIC's effect on privacy. Those concerns included a lack of due process against government searches; unregulated Identity Providers; no mandatory adherence to Fair Information Practice Principles (FIPPs), and others. One NIST official thoughtfully listened to and responded to each concern. In addition to some very thoughtful responses, the NIST official counter-argued that each problem was already

[11] *National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy*, April 15, 2011, p. 24. http://www.nist.gov/nstic.

[12] Luma Partners, LLC has produced a vivid slide demonstrating the Display Advertising Technology Landscape, dated March 15, 2011. A copy of that slide is available at http://www.slideshare.net/tkawaja/luma-display-ad-tech-landscape-2010-1231 (Accessed March 28, 2011).

[13] Improve Digital, *2010 – Display Advertising Market Map Europe—v. 1.1, English*, http://www.improvedigital.com/wp-content/uploads/DigitalAdvertisingIndustryMap2010_EN_1.2.pdf (Accessed March 28, 2011).

occurring in the present system, independent of NSTIC. He re-framed the discussion by suggesting that NSTIC, even in its worst possible implementation will be no worse than the status quo trajectory of privacy in the United States. He argued that with no down-side to privacy and only potential benefits, NSTIC should be adopted. In other words, NSTIC will have a net zero or positive effect on privacy.

This is an intriguing argument. Let's assume, for argument's sake, that privacy practices in the United States are following a trajectory which could be coarsely described by the graph in **Figure 3**.

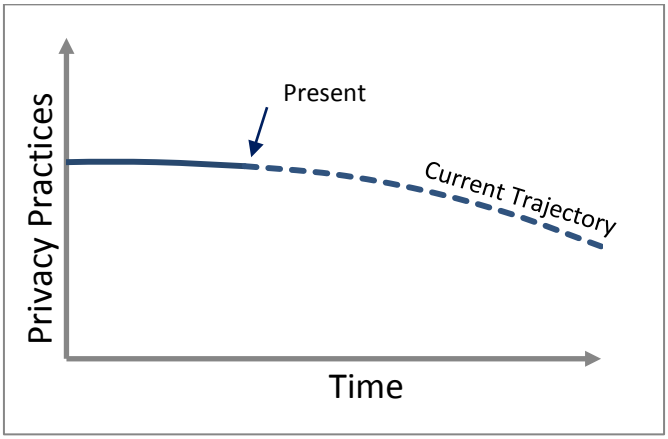

Figure 3: Roughly Projected Privacy Practices Over Time

The argument that NSTIC can do no more harm to privacy practices than our current path is hardly comforting, but is perhaps the single most logical and compelling argument in favor of implementing NSTIC. Any logical person would agree that one should adopt a system which can do no harm to privacy, while creating significant economic benefits.

Thus, it is prudent to investigate the NIST official's claim that NSTIC can create no more harm to privacy than will already occur in the inevitable future. This report concludes that despite NSTIC's vision of privacy, success is far from assured. NSTIC will create new tools which will permit Ecosystem Participants to enhance or erode privacy. The tools, without the proper rules, to paraphrase Scott David, will be abused. As NSTIC does not currently propose legislation or regulation, it is far from certain that sufficiently privacy-enhancing rules will be developed or that they will have the force and effect of law. This means that NSTIC's worst (or even realistic) case could theoretically be worse than the status quo, as illustrated in **Figure 4**.

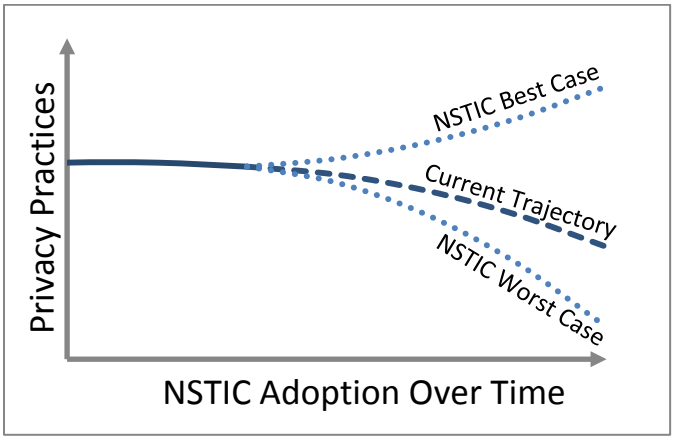

Figure 4: Possible NSTIC Effects on Privacy. NIST Argues that NSTIC can Have Only a Net Positive Effect on Privacy, no Worse than the "Current Trajectory"

Core Ecosystem Roles and Definitions

The Identity Ecosystem Marketplace includes at least six major roles, as illustrated in **Figure 5**. We review the roles here, and will explore various interactions among these roles in this report. A single organization may fill multiple roles in any given Identity Ecosystem transaction.

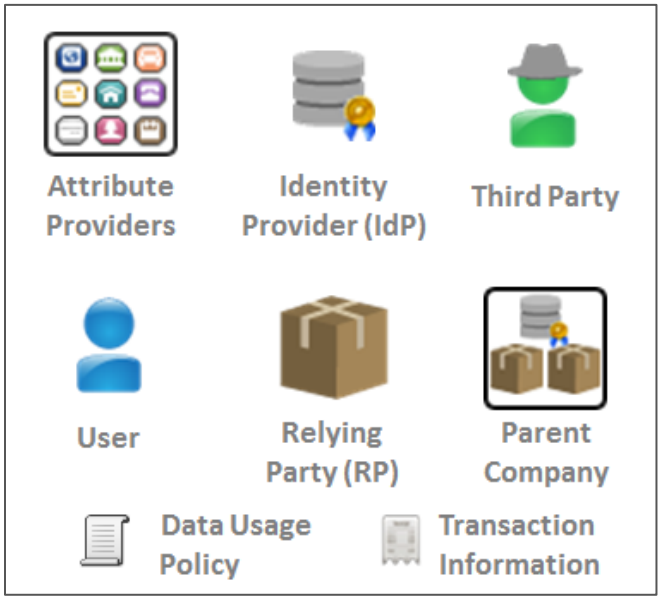

Figure 5: Major Identity Ecosystem Roles and Concepts

A **User** or Subject is a person or Non-Person Entity (NPE) which must assert its identity to a Relying Party in order to receive a benefit such as access to a trusted network, bank account access, or access to premium content online.

An **Attribute Provider** (AP) creates, stores and allows others (such as the Identity Provider and Relying Party) to access or analyze User Attributes, usually under conditions. An Attribute Provider is also usually a Third Party. In the Identity Ecosystem, an Attribute Provider must be trusted as an authoritative source of information. Typical examples of attribute providers might be a government title registry, national credit bureau, or commercial marketing database.

An **Attribute** is a fact related to a User. Attributes may include traditional PII, information about authority, roles, rights, privileges, or any other fact asserted by a User, Attribute Provider, or Third Party.

An **Identity Provider** (IdP) is an organization certified as trustworthy through an accreditation authority. An IdP issues a credential, which corresponds to a piece of information known to the User (such as a password), a biometric attribute, or information stored on an Identity Medium (not represented herein). An IdP is responsible for verifying the credential when used as evidence of a User's identity. An IdP may collect attributes about the User from Attribute Providers, store those attributes, and compare them against assertions made by the User to a Relying Party. Identity Providers do not guarantee the correctness of attributes obtained from Attribute Providers, but may instead confirm that a Claim made by a User matches information from Attribute Providers. Identity Providers may share User attributes, personal information, and Transaction Information with Relying Parties, Third Parties, Parent Companies and Attribute Providers, in accordance with the Data Usage Policy.

A **Data Usage Policy** is a contract between a User and Identity Provider, governing the use and disclosure of User information held by the Identity Provider.

Transaction Information is a record of the benefit provided to the User from the Relying Party, and is analogous to a receipt. Transaction Information may include the name of a product purchased, a log of network access and User activity, or services provided.

Identity Medium refers to the physical device that stores an NSTIC-compatible identity credential. Examples of Identity Mediums include cell phone apps, smart cards, or computer dongles. Identity Media are not visually represented in this report, and are not required for a transaction.

A **Relying Party** (RP) is a person or NPE that requires some degree of identity assurance and possibly User Attributes before it will provide a benefit to the User.

A **Parent Company** is a company which owns or is affiliated with the Identity Provider and/or the Relying Party in such a way that by action of law, ownership or contract, the Parent Company has right to access and use the Identity Provider or Relying Party's data assets, unless expressly prohibited by law or regulation.

A **Third Party** is any person, organization, system, or device which has no direct affiliation with the User or the transaction in question. A familiar example of a Third Party is an online advertiser.

For purposes of this report, we define a **Claim** as an assertion that an Attribute is truthful or correct. A Claim may be made by any party. Examples of User Claims are, "I am over 18 years old," "I am a constituent or citizen," or "I am authorized to enter your network." Claims are not visually represented in this report. In technical circles, a "claim" is an assertion that may be derived by comparing or analyzing one or more Attributes.

According to NSTIC, the **Identity Ecosystem Framework** is "the overarching set of interoperability standards, risk models, privacy and liability policies, requirements, and accountability mechanisms that structure the Identity Ecosystem."[14]

The **Identity Ecosystem Marketplace** is the Identity Marketplace created by the Identity Ecosystem, where Identity Ecosystem Participants may commoditize and trade User identities and Attributes in exchange for benefits. Not all Identity Ecosystem transactions necessarily commoditize human identity. The exchange of identity information in many e-commerce transactions is ancillary to the transaction, and the User pays directly for the benefit of the transaction (e.g. a money transfer, music or movie download). Notwithstanding, the Identity Ecosystem Marketplace enables Participants to more easily commoditize identity as an additional source of revenue.

Fair Information Practice Principles (FIPPs) are Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing. NSTIC identifies FIPPs as core requirements in the Identity Ecosystem, but stops short of mandating FIPPs.

[14] *National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy*, April 15, 2011, p. 24. http://www.nist.gov/nstic.

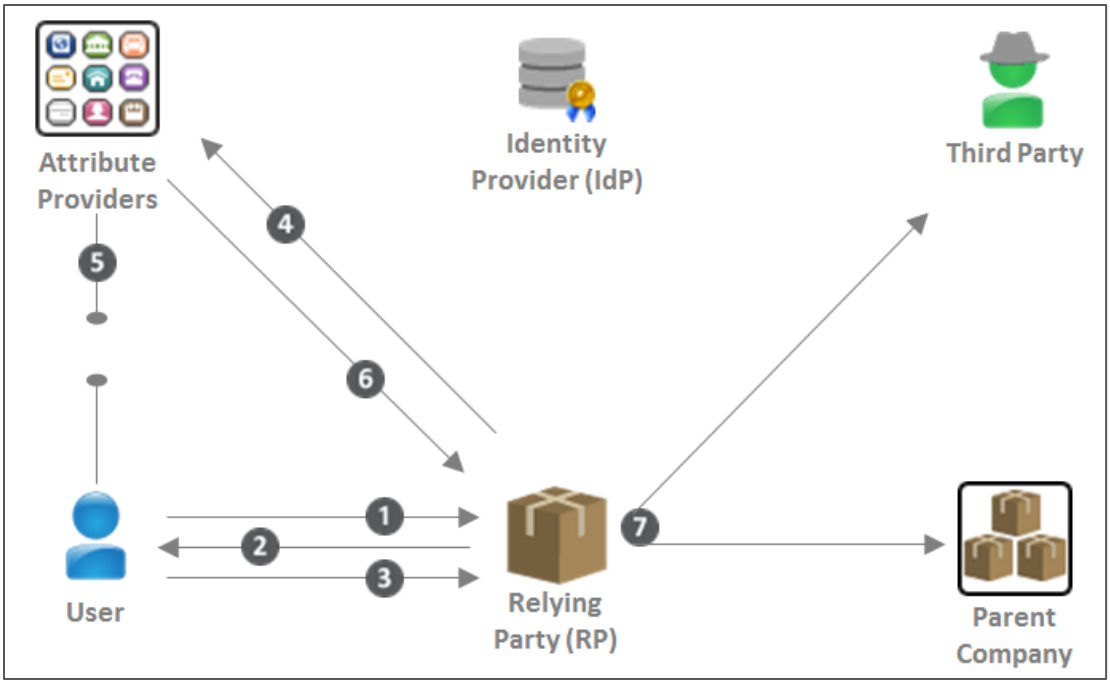

Figure 6: Current Typical Verified Transaction (Communication Diagram)

Verified transactions occur between consumers and service providers even today. A simplified verified transaction today is illustrated here. In this example, the Relying Party could be an online service provider, while the Attribute Provider could be a Credit Reporting Agency. In **Figure 6**, the numbers and lines represent the following communications among Participants:

1. The User requests a service or benefit from the Relying Party
2. The Relying Party requests personal information, such as a SSN and other Personally Identifiable Information (PII)
3. The User provides his SSN and PII to the Relying Party
4. The Relying Party sends the SSN and PII to an Attribute Provider
5. The Attribute Provider rarely has a duty to ask the User permission to share additional PII with the Relying Party or Third Parties.
6. The Attribute Provider verifies that the SSN and PII match its records, and may send additional information, such as a credit score to the Relying Party.
7. The Relying Party provides the benefit, and absent fiduciary or contractual limitations, may share the SSN and PII with its Parent Company and Third Parties.

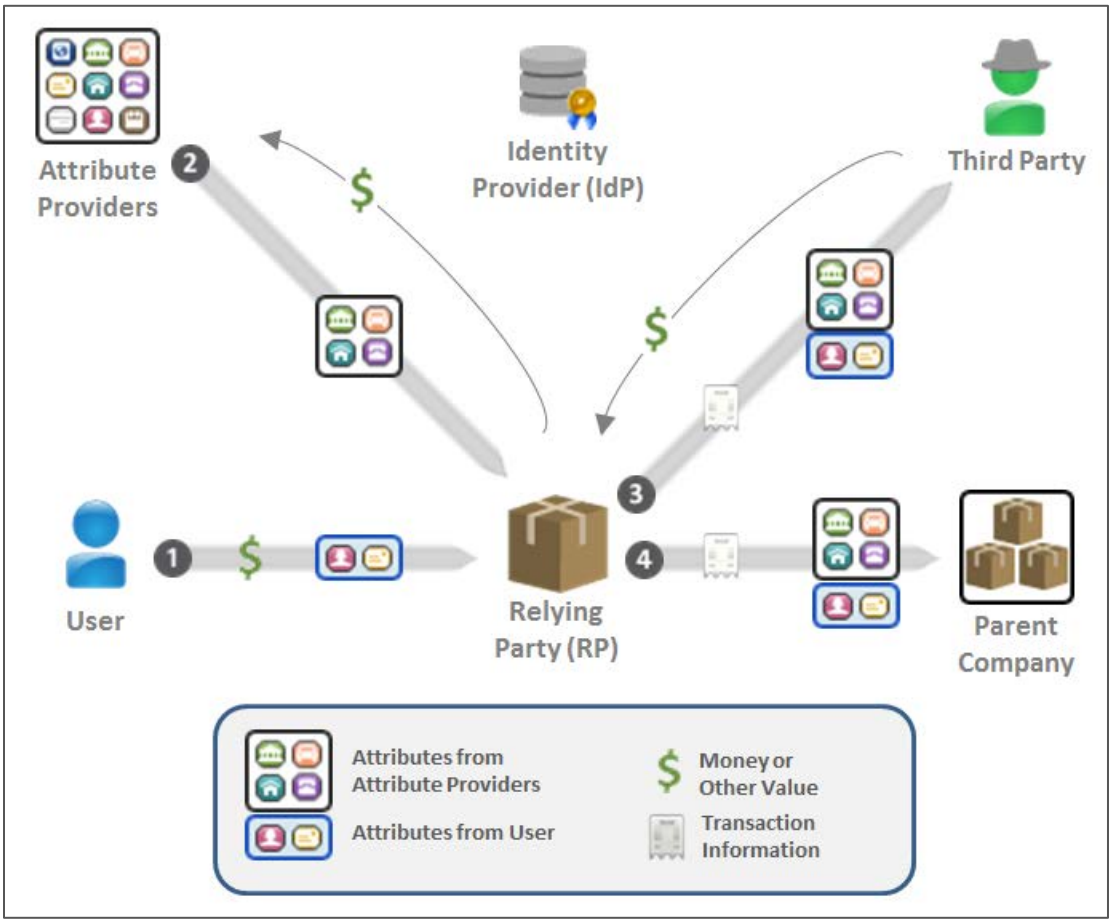

Figure 7: Current Typical Verified Identity Transaction (Identity Market Diagram)

Verified transactions occur between consumers and service providers daily. This transaction illustrates the same transaction as **Figure 6**, but instead illustrates the exchange of data and money or value. In this example, the Relying Party could be an online service provider, while the Attribute Provider could be a Credit Reporting Agency. In **Figure 7**, data and money (or other value) is typically exchanged in the following manner during a verified identity transaction:

1. The User provides the Relying Party some small set of personal Attributes, as well as money or value in exchange for a benefit.
2. Attribute Providers give the Relying Party additional User Attributes, in exchange for money or value.
3. Absent fiduciary or contractual limitations, the Relying Party may aggregate and share the User Attributes and Transaction Information with third parties, in exchange for money or value.
4. The Relying Party is often required to share Transaction and aggregated User Attributes with its Parent Company.

Current Typical Verified Transaction

Already today, verified transactions occur on and offline between consumers and service providers (see **Figure 6**). For example, when an individual enters into a contract with an online service provider (the Relying Party), the provider may require the User to divulge sensitive personal information, such as a social security number (SSN). The company may use the SSN to check the User's credit score and home address against a credit bureau such as Equifax (the Attribute Provider). Once the Attribute Provider verifies the User's credit score, the service provider grants a benefit to the User (e.g., access to financial resources). A typical verified transaction today is illustrated in **Figure 6**, simplified for clarity.

Most federated identity diagrams describe communications and protocols, much like **Figure 6**. In order to analyze market forces, risks, and motivations driving NSTIC technology, it is necessary to examine identity transactions in terms of data and money exchange. **Figure 7** illustrates the same transaction as **Figure 6**, ignoring individual communications and technical protocols. **Figure 7** analyzes only the exchange of data and money among the roles in the Identity Ecosystem Marketplace.

A few interesting points emerge from **Figure 7**. Most importantly, the Relying Party is the center of the current Identity Market, and controls the exchange of attributes and money. Although most Relying Parties are not "Identity Oracles,"[15] they do derive value from the User's personal information, and have a financial incentive to keep the information, and their reputations safe. The value of User personal information includes marketing value, and cash value when it is sold to third parties.

Despite damage to reputation, increasing remediation costs,[16] and regulations requiring security and breach notifications, breaches of personal information from Relying Parties continue to occur at alarming rates.[17] Breaches have multiple causes, including mishandling of storage devices, hacking, dishonest insiders, and negligence. Regardless of the precipitating factors leading to breaches, the sheer number of them indicate that market forces do not yet value personal information sufficiently to warrant investment to secure those Attributes.

Ideal Federated Identity Transaction

NSTIC seeks to improve security by formalizing an additional role into the Identity Ecosystem, the Identity Provider (IdP). According to NSTIC, an IdP is responsible for "establishing, maintaining, and securing the digital identity associated with [a] subject." The IdP is responsible to issue credentials, and revoke compromised credentials.[18]

Identity Providers already exist. Companies like Google, Facebook and Twitter allow you to use their credentials to log into other websites, with varying degrees of security and privacy. Currently, Identity Providers are largely unregulated. In this respect, NSTIC represents an opportunity to adopt standards that would improve their privacy practices.

Figure 8 outlines an ideal verified federated identity transaction that utilizes privacy-enhancing technology, zero-knowledge proofs, and implements generally accepted FIPPs, including data minimization.

Figure 9 analyzes the same transaction in terms of the exchange of data and money among the Identity Ecosystem roles in the Identity Ecosystem Market. (*continued on pg. 19...*)

[15] As defined by Bob Blakely, an "Identity Oracle" is "An organization which derives all of its profit from collection & use of your private information... And therefore treats your information as an asset... And therefore protects your information by answering questions (i.e. providing meta-identity information) based on your information without disclosing your information... Thus keeping both the Relying Party and you happy, while making money." This report contains more discussion about Identity Oracles below. See Bob's 2006 presentation on the subject at http://podcast.burtongroup.com/ip/2006/06/identity_and_co.html, and an informative follow-up blog post here: http://identityblog.burtongroup.com/bgidps/2007/10/what-the-identi.html

[16] The Ponemon Institute publishes annual statistics on the cost of breaches. Links to their statistics and white papers may be found at: http://www.ponemon.org/data-security

[17] *See, e.g.*, the Open Security Foundation's Data Loss DB, http://datalossdb.org/. See also the Identity Theft Resource Center's Report, *Date Breaches: The Insanity Continues*, http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2009_Data_Breaches.shtml

[18] *National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy*, April 15, 2011, p. 21. http://www.nist.gov/nstic.

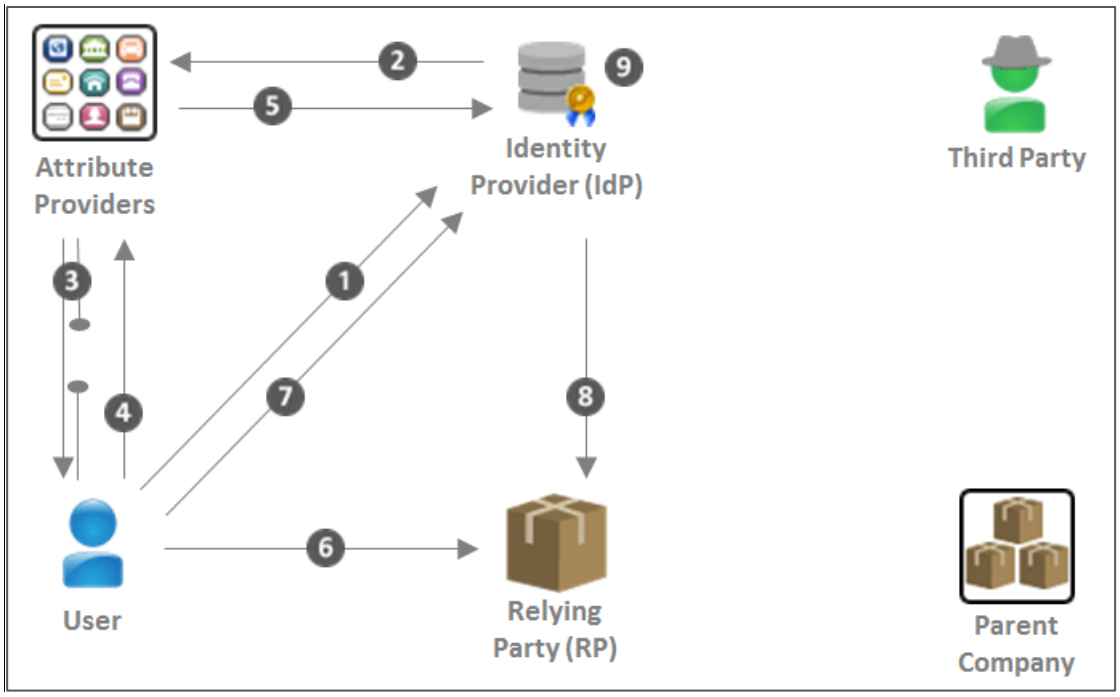

Figure 8: Ideal Federated Identity Transaction (Simplified Communication Diagram)

Figure 8 outlines an ideal verified federated identity transaction that utilizes privacy-enhancing technology, zero-knowledge proofs, and implements generally accepted FIPPs, including data minimization. In this simplified communications diagram, an ideal Federated Identity Transaction would include the following steps:

1. The User contacts the Identity Provider, and dictates the terms of the Data Usage Policy to the IdP, which the IdP accepts. The User then provides PII to the Identity Provider.
2. The IdP may contact Attribute Providers, requesting that the Attribute Provider confirm the User's Attributes, and perhaps share additional Attributes.
3. Ideally, an Attribute Provider will a duty to ask the User's permission to share or confirm attributes. However, this will not always be the case. For example, while a healthcare clearinghouse may be required to get consent to share Attributes, an online marketing agency may not.
4. However, in the rare event that an Attribute Provider must ask consent, the User would provide it.
5. The Attribute Provider verifies the User's PII to the IdP.
6. Later, the User requests a service from a Relying Party. The Relying Party must know certain Attributes about the User before it can provide a benefit. Instead of giving the Relying Party his date of birth, the User asserts that he is over 18 years old.
7. Ideally, the User does not share his NSTIC credential with the Relying Party, but transmits it directly to the IdP, with no information about the transaction.
8. The IdP transmits a message to the Relying Party, verifying the User's identity.
9. In a zero-knowledge transaction, the IdP would have no knowledge of the details of the transaction.

This implementation of NSTIC creates a better privacy outcome than the current trajectory of privacy practices in the United States.

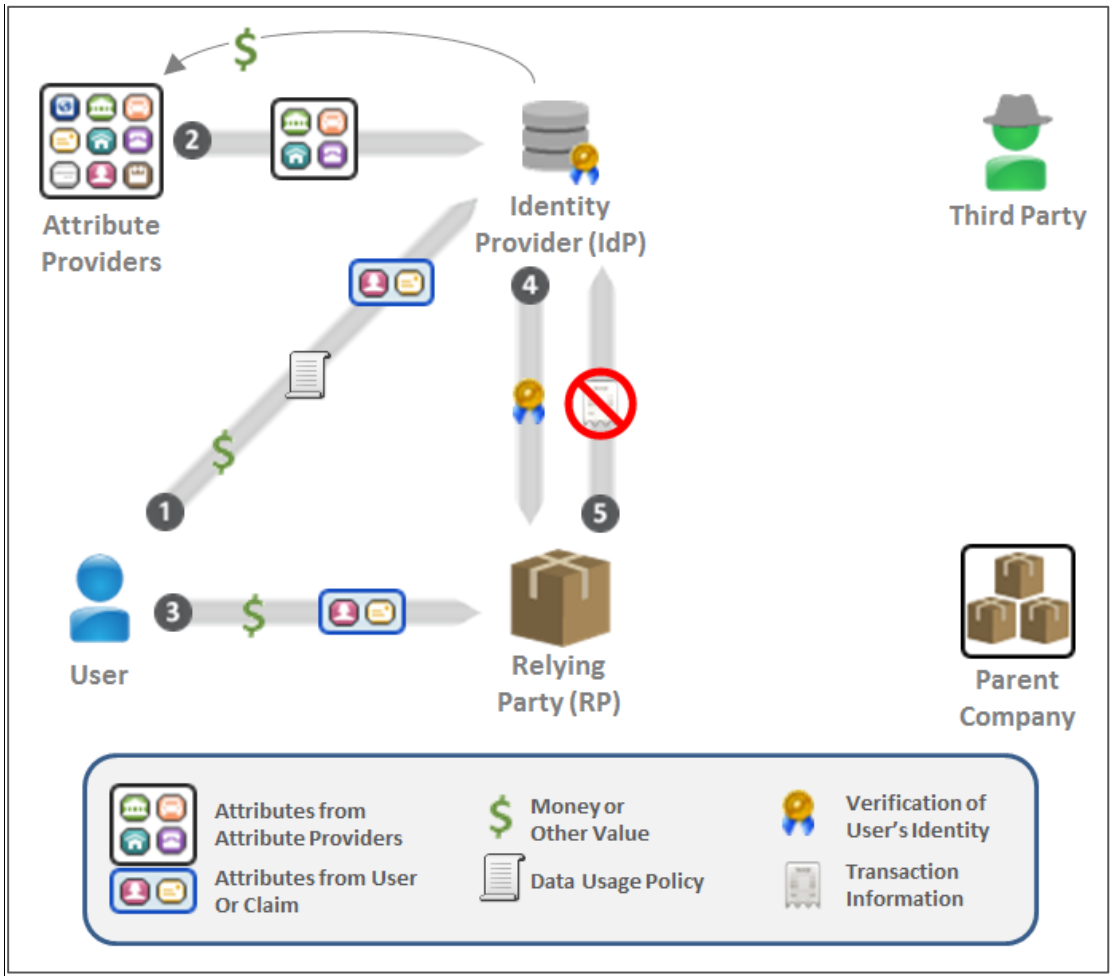

Figure 9: Ideal Federated Identity Transaction (Identity Market Diagram)

Figure 9 analyzes the same transaction as **Figure 8**, in terms of the exchange of data and money among the Identity Ecosystem Market participants. In this Identity Ecosystem Market diagram of an Ideal Federated Identity Transaction, the exchange of data and money would proceed as follows:

1. The User gives the Identity Provider a limited amount of personal information, and money or other value for the IdP's service, then dictates the terms of the Data Usage Policy, which the IdP accepts.
2. Attribute Providers may provide additional attributes to the IdP in exchange for money or value.
3. The User gives the Relying Party a limited amount of personal information in the form of a Claim. The User may also pay the Relying Party money for the benefit.
4. Instead of providing personal information to the Relying Party, the Identity Provider certifies that the User's Claim is true.
5. The Identity Provider may have limited or no knowledge about the transaction between the User and Relying Party, depending upon the technology used.

This implementation of NSTIC creates a better privacy outcome than the current trajectory of privacy practices in the United States.

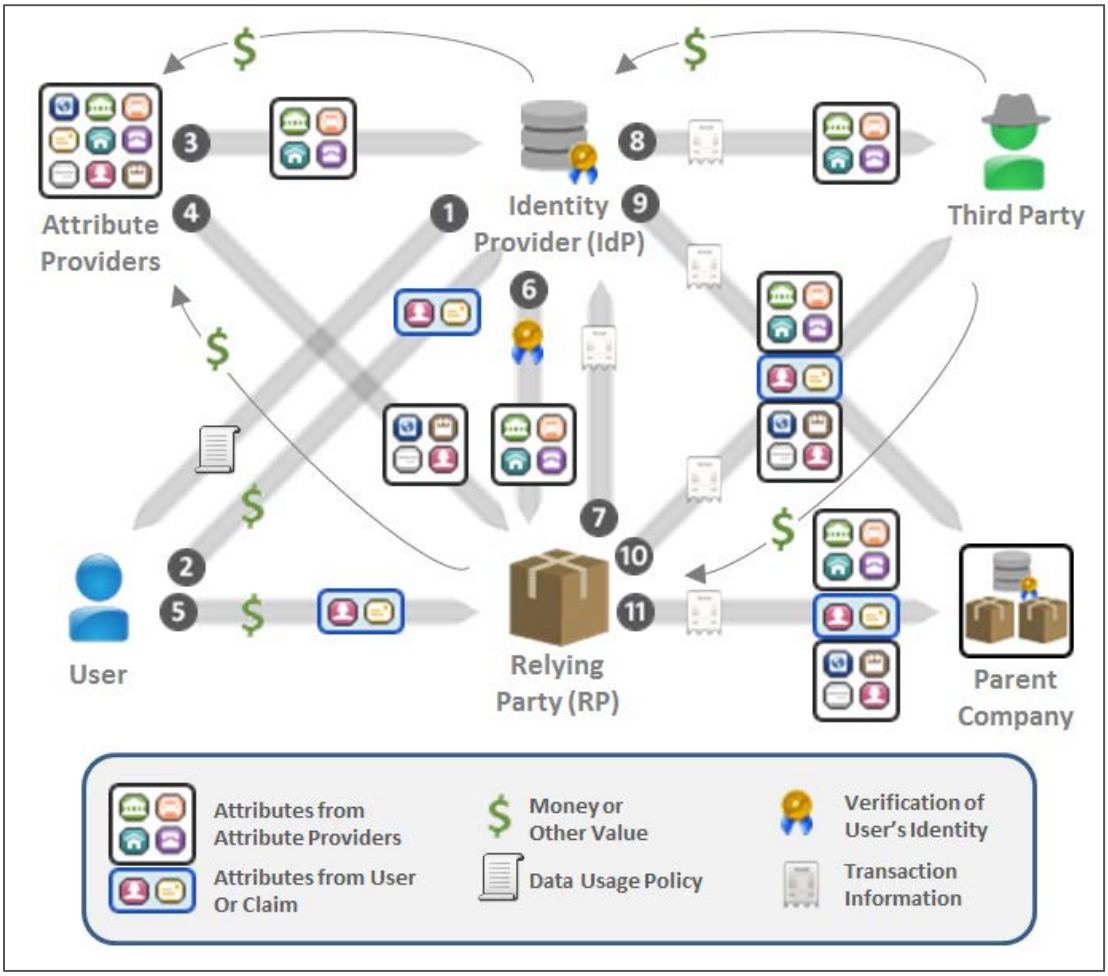

Figure 10: Realistic NSTIC Data Transaction (Identity Market Diagram)

Even though the following scenario sharply conflicts with the aspirations of NSTIC, without proper policy restrictions, a likely Identity Ecosystem Marketplace transaction would proceed much like a transaction today, but with more opportunities to buy and sell data:

1. As a condition of service, the IdP dictates the Data Usage Policy to the User, which the Identity Provider to maximize the economic value of the User's personal information.
2. In exchange for services, the User accepts the Data Usage Policy and provides the IdP with money or other value for the IdP's service, along with personal information
3. Attribute Providers may provide additional Attributes to the IdP in exchange for money or value.
4. In exchange for a benefit, the User gives the Relying Party a limited amount of personal information in the form of a Claim. The User may also pay the Relying Party for the benefit.
5. In order to maintain a needed source of income, the Relying Party may purchase additional User Attributes from Attribute Providers, which it may then enrich with Transaction Information and sell to Third Parties (see #10). Relying Parties may purchase additional information from Attribute Providers, even in an ideal implementation of an NSTIC Federated Identity System. Relying Parties may use this information for financial gain, or sharing may be

practically necessary for highly variable Attributes which cannot be reliably stored with the IdP (e.g., GPS location data).

6. The Relying Party requests the IdP to confirm the User's Identity, and the IdP verifies the identity and provides additional User personal information to the Relying Party as permitted by the Data Usage Policy. This transaction might be facilitated by trading Transaction Information for User Attributes (see #7), or the Relying Party and Identity Provider may be owned by the same Parent Company (see #9 and #11); or the Relying Party and IdP may have some other affiliate agreement.
7. The Relying Party shares Transaction Information with the IdP, and may share money or other value.
8. In accordance with the Data Usage Policy, the IdP can enrich the User Attributes with Transaction Information which it may sell to Third Parties.
9. The IdP shares all User Attributes and Transaction Information with its Parent Companies and Affiliates.
10. The Relying Party may share all User Attributes and Transaction Information with Third Parties.
11. The Relying Party shares all User Attributes and Transaction Information with its Parent Companies and affiliates.

Because Identity information is traded more widely, this implementation of NSTIC creates a worse privacy outcome than the status quo represented by **Figures 6** and **7**.

(*...continued from pg. 14*) In order to operate in the manner illustrated in **Figures 8** and **9**, the Ideal Federated Identity Transaction makes one fundamental assumption: *The User will dictate the terms of the Data Usage Policy*. If the User is able to choose the terms of his Data Usage Policy, he will no doubt protect his personal information or make an informed choice to exchange it for benefits.

NSTIC envisions an Identity Ecosystem where Data Usage Policies are written with the interests of the User in mind, but it is unclear how NSTIC will accomplish this goal. Given unequal bargaining power between the IdP and User, the Data Usage Policy will more likely be dictated to the User on terms favorable to the IdP's business interests. And much like today's corporate Privacy Policies, Identity Ecosystem Data Usage Policies will likely be a condition of service, offered on a take-it-or-leave-it basis.

Further, as **Figure 9** demonstrates, an ideal Federated Identity Transaction will displace the Relying Party from its centralized role in the Identity Market, and replace it with a competitor, the Identity Provider. This market shift has already begun to occur, in part due to the enriched personal information IdPs can provide Relying Parties about their Users. Coaxing Relying Parties to trust the assertions of an IdP is the subject of a considerable amount of work and research. Aside from issues of trust, this diagram raises the question why a Relying Party would willingly relinquish control of User personal information, in light of its accompanying cash stream.

One could argue that the cost of securing personal information exceeds its value, and that Relying Parties will gladly rid themselves of sensitive and non-sensitive User attributes as a liability rather than an asset. If that were the case, one would expect companies to have already secured sensitive personal information using third parties who specialize in security. However, daily reports of breaches, and the sheer number of organizations which collect and store personal information indicate that has not happened. The potential liabilities of storing personal information do not yet equal the costs of properly protecting it. Relying Parties have more incentive to retain and store personal information, and its associated cash stream, than give up this right to an IdP.

However, Relying Parties will willingly relinquish their centralized role in the Identity Ecosystem Marketplace if IdPs are able to replace the value lost from identity information with something of equal or greater value. In addition to ease of use, too often IdPs offer Relying Parties enriched behavioral data about their Users, which is of greater value than information the Relying Party could collect on its own.

Likely NSTIC Data Transaction

In contrast to **Figure 9**, **Figure 10** illustrates the likely exchange of data and money among Identity Ecosystem Marketplace Participants in a typical NSTIC Data Transaction. Even though the scenario sharply conflicts with the aspirations of NSTIC, this type of transaction is likely to occur in an unregulated Identity Ecosystem Marketplace.

As illustrated by comparing **Figures 9** and **10**, the identity Ecosystem will create new ways to trade personal information. Unless moderated by policy and regulations which enforce the intentions and aspirations of NSTIC, the Market will encourage Participants to increase the flourishing trade of human identities and substantially decrease "wholesale" privacy.

Even an unregulated Identity Ecosystem Marketplace may improve "retail privacy"—that is, NSTIC may decrease the amount of information shared between the User and Relying party (see **Figure 10**, #4)—but will have a deleterious effect on "wholesale privacy," since the Identity Provider will be able to share personal information with Third Parties and often the very Relying Parties from whom the User is trying to keep it. This is why regulation enforcing NSTIC's vision is vital.

Roles of Technology, Policy, and Market Forces

Relevant to the present discussion, three great forces will shape the future of identity and privacy: Market forces, Policy forces, and Technology. For purposes of this report, "Market" forces are defined broadly and include all social, economic, behavioral and other forces which drive the actions of individuals and organizations. "Policy" is similarly broad, and includes formal law, regulation, and government intervention generally.

We will analogize Market and Policy forces to two train engines, and analogize technology to the train track on which the engines run. While the engines may pull together or apart from one another, the technology enables and places limits on these two great forces as they awkwardly interact, as illustrated in **Figure 11**.

Technology Enables Policy and Markets to Achieve Goals

In this analogy, technology is no passive participant. After all, the engines of Market and Policy are bound to the paths technology chooses to take it. Without the enabling technology, Google's business plan would have failed in 1950. Similarly, wiretap laws would have had no meaning without Alexander Graham Bell's invention, the telephone.

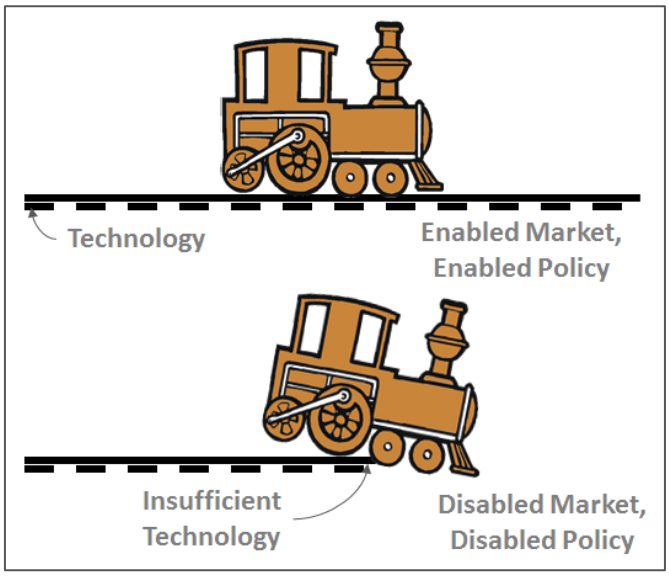

Figure 11: Technology Enables Markets and Policy

Lawrence Lessig expressed a similar idea in his famous essay, *The Code Is the Law*.

> "The single most significant change in the politics of cyberspace is the coming of age of this simple idea: The code is law. The architectures of cyberspace are as important as the law in defining and defeating the liberties of the Net. Activists concerned with defending liberty, privacy or access must watch the code coming from the [Silicon] Valley - call it West Coast Code - as much as the code coming from Congress - call it East Coast Code.... Let them [each] publish their regulations, so the regulated can choose." [19]

Ideal Interactions Among Technology, Policy, and Market Forces

While Technology may enable and set bounds to Policy and Market forces, technology cannot mandate the direction these forces will go. A hammer cannot determine whether it is used for construction or demolition. Automobiles cannot avoid injuring a pedestrian in the hands of a negligent driver. A light bulb cannot turn itself on or off. Technology can no more create market forces, nor unilaterally solve policy problems than a track can force a train to travel forward or backward.

Ideally, technology, policy, and market forces will work together to reach a point of maximum benefit. Maximum benefit may not mean "no harm," and of course, defining "maximum benefit" is an ongoing subject of debate among economists, philosophers, and politicians to name a few.

Notwithstanding the rhetorical difficulties posed by the term "maximum benefit," **Figure 12** illustrates two Ideal interactions among Technology, Policy, and Market forces. If the maximum benefit requires effort in a single direction, then the Market and Policy should work together in the same direction to reach the maximum benefit. In contrast, if the maximum benefit requires balancing two or more ideals, then Policy and Market forces should exert some degree of tension on one another to achieve the proper balance of interests.

[19] *The Code Is the Law*, April 9, 1999. http://www.lessig.org/content/standard/0,1902,4165,00.html (Accessed March 28, 2011).

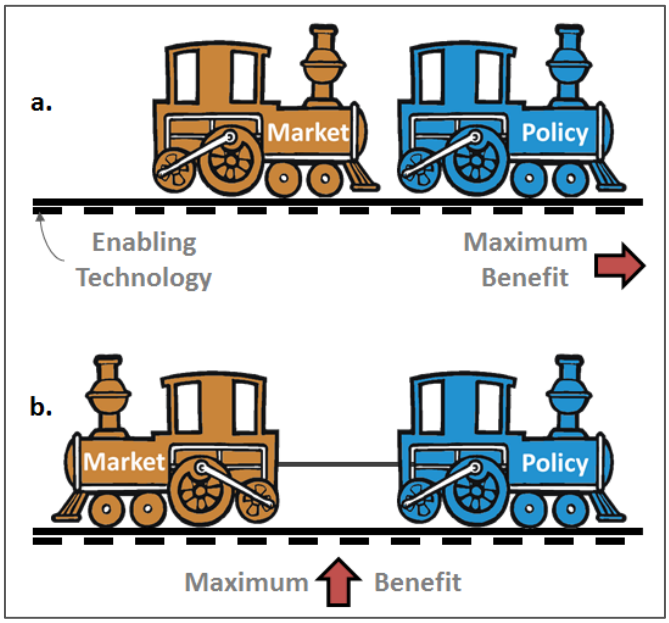

Figure 12: Two Ideal Interactions Among Enabling Technology, Market Forces, and Policy

The opposite of an ideal interaction among Technology, Policy, and Market forces is the instance where Policy and Market forces work together, counteractive to the maximum benefit, as illustrated in **Figure 13**.

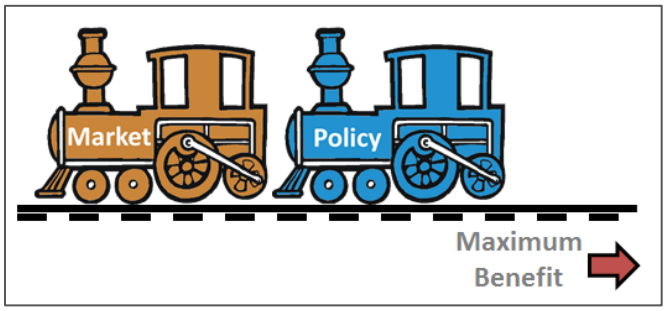

Figure 13: Faulty Interaction Among Technology, Market Forces, and Policy, Away from the Maximum Benefit

Figures 11-13 suggest the questions,

- **What possibilities do NSTIC technologies enable?**
- **What is the maximum benefit enabled by these technologies?**
- **How will the Identity Ecosystem Marketplace utilize the technology?**
- **Does NSTIC policy provide tension against or reinforcement to Market forces?**
- **Is the resulting interaction among NSTIC Policy, Market Forces and Technology *ideal* or *faulty*?**

Analysis of NSTIC Technology and Identity Ecosystem Market Forces

Technology Vulnerabilities Not Analyzed

The technological challenges associated with implementing a nation-wide secure framework of privately-owned, interoperable federated identity systems *cannot be understated*. Major security breaches strike at core protocols of the Internet on almost a monthly basis. We must acknowledge that the technology layer can never eliminate risk from the human layer of the networked world. Even secure technologies can be broken by a determined adversary.

This report does not analyze the efficacy of technologies or protocols, nor does it address technological security vulnerabilities. Examples of technological security risks may include: Encryption vulnerabilities, DNS spoofing, and phishing attacks to name a few. All scenarios examined in this report may be accomplished without bypassing technological protocols designed to prevent fraud.

NSTIC envisions a process for developing a secure Identity Ecosystem which will require developing and adopting standards and policies over a period of years. For the purposes of this report, we assume that all of the myriad technological challenges associated with implementing a large-scale federated identity system, such as NSTIC, will be addressed prior to launch.

NSTIC Technology Enables Identity Sharing or Hoarding

NSTIC is a policy, not a technology. From an Identity Marketplace perspective, federated identity technology can be implemented to *share* or *hoard* identities and personal information. "Sharing" includes trading, selling, renting, licensing and giving; while "hoarding" simply means that the identity information is not traded, sold, rented, licensed or otherwise shared with another party.

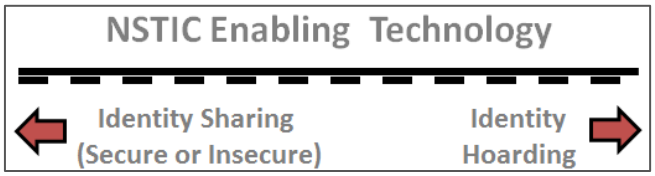

Figure 14: Federated Identity Technologies Enable Data Sharing (Secure or Insecure), or Data Hoarding

The dichotomy between "share" and "hoard" should not be mistaken for "secure" and "insecure." As technologists in this field know, both sharing and concealing may be done in secure or insecure manners. For the purposes of this report we will take a large leap of faith and assume that all identity information will be shared or stored using secure technological and business processes. Implementing security protocols in a business environment is a subject for a different report.

Identity Sharing is Profitable; Hoarding Improves Privacy

Since identities and personal information have value, trading and sharing identities generally yields profit while the very act of sharing decreases privacy.[20] In contrast, while hoarding identity information improves privacy, it is not profitable in most circumstances.

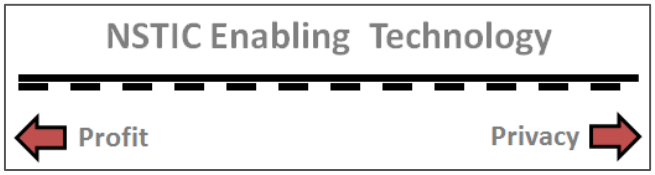

Figure 15: NSTIC Enables Profit or Privacy

This thesis is supported by even a cursory look at current market conditions. Data and identity aggregation is a multi-billion dollar business and it is almost axiomatic to say that neither Google nor Facebook's combined $200+ Billion market capitalization was amassed by keeping personal information private.

Federated Identity technology enables sharing or hoarding, or in other words, profit or privacy. All business models have one thing in common: They favor profit, as illustrated in **Figure 16**:

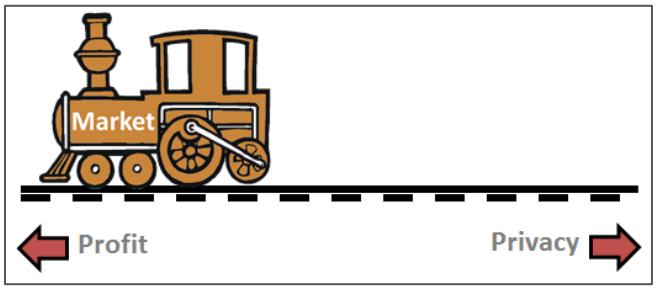

Figure 16: Market Forces Favor Profit

We note that some entrepreneurs have developed innovative and (unfortunately) niche business models which make privacy profitable. We applaud and encourage companies to develop business models that make money by improving privacy and do not depend upon the commoditization of human identity. We also note, however, that notwithstanding these pioneering business models, identity trading remains a multi-billion dollar industry, and a primary threat to individuals' privacy and security.

NSTIC Policy Should Create Tension Against Market Forces to Balance Profit and Privacy

We believe that Privacy is worth protecting; and we understand that businesses must be profitable. Therefore, to obtain the maximum benefit NSTIC Policy and Market forces must balance the interests of profit and privacy. As illustrated in **Figures 12b** and **17**, this means that NSTIC Policy should create some tension with Market forces.

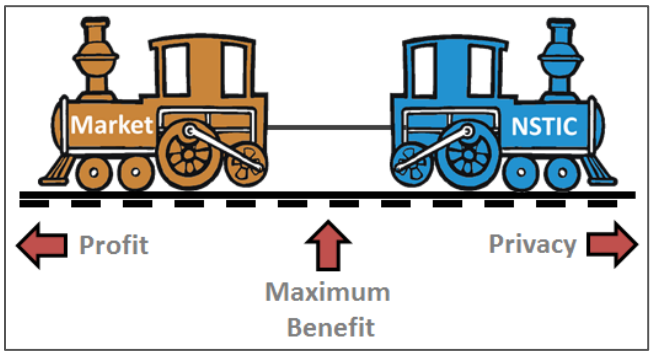

Figure 17: NSTIC Policy Should Create Tension with Market Forces to Obtain the Maximum Benefit—Balance Between Privacy and Profit.

[20] A User may consent to identity sharing. Consent to eliminate privacy does not improve privacy; consent simply authorizes decreased privacy.

Analysis of NSTIC Policy

With this background, this section will now analyze NSTIC Policy's effect on privacy within the context of Market forces and enabling technology, and explore whether NSTIC creates the necessary tension with Market forces to balance profit and privacy

NSTIC Policy Looks the Right Direction, but Lacks Force

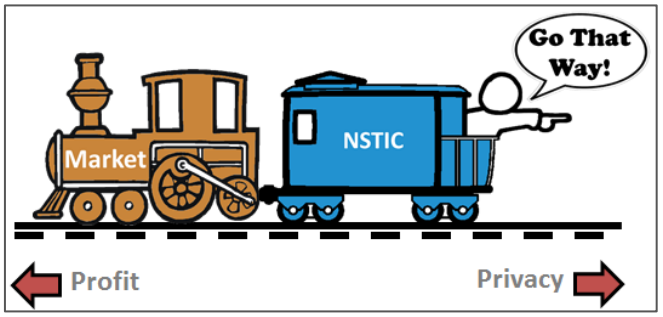

Figure 18: NSTIC Envisions Privacy, but Does Not Yet Envision a Regulatory Framework to Make it Real.

NSTIC implementation policy must take concrete regulatory steps to balance profit and privacy.

Even though privacy-enhancing technology exists, without the proper policy, law, and regulatory safeguards in place from the outset, Market forces will reject or misuse these technologies. Profit-oriented businesses would be incentivized to use the NSTIC framework as a tool to obliterate privacy, anonymity and its attendant liberties, in all but the fewest of circumstances. NSTIC aspires to privacy, but does not yet have the force to make its aspirations a reality. In short:

- The Market won't protect privacy.
- Technology can't create Policy.
- NSTIC Policy must protect privacy, but doesn't (yet).

Unsolved NSTIC Policy Hurdles

If NSTIC is to accomplish its vision, future regulations must address a range of severe policy vulnerabilities which remain unsolved. These security risks do not entail circumventing technology, but rather are technology-independent. As a result, these problems cannot be solved through technology alone; policy problems must be solved through better policy.

Without regulatory mandates that require IdPs and Relying Parties to follow minimum standards for privacy-enhancing technologies or basic security, these Market Participants will have multiple incentives to behave in ways detrimental to Users' Privacy. For reasons discussed in detail above, the Market is not likely to self-regulate best practices into their business processes.

Identity Finder has identified the following unresolved Policy hurdles in an unregulated Identity Ecosystem Marketplace, which are discussed below:

- FIPPs May not be a Silver Bullet
- Data Usage Policies will Favor IdPs or Relying Parties, Not Users' Privacy
- Identity Providers will Create Centralized Databases of Personal and Transaction Information
- Identity Providers Must Be Regulated
- User Rights will End Upon Data Policy Deletion
- Identity Credentials will be an Internet "Power of Attorney" Without Procedural Safeguards
- NSTIC Credentials will Create New Identity Theft Vectors
- Unregulated Relying Parties May Use NSTIC IDs to Over-Identify Users
- NSTIC Must Provide Recourse to Correct False Information or Damage to Reputation

FIPPs May not be a Silver Bullet

The Fair Information Practice Principles (FIPPs) are core principles of the Privacy Act of 1974 in the United States and have been almost universally adopted by other governments, businesses and organizations. FIPPs are not mandated by NSTIC.

NSTIC makes multiple references to the importance of FIPPs in a secure, trusted identity framework. We support this idea, but warn of the need to implement FIPPs strictly and contextually.

Even though FIPPs have attained international acceptance, consistently applying FIPPs is notoriously difficult. For example, the Department of Homeland

Security (DHS)[21] has adopted FIPPs as a matter of policy.[22] Yet the DHS's Privacy Office found that even the extremely controversial Whole Body Imaging technology complies with all FIPPs.[23] Google has adopted a subset of Fair Information Practice Principles,[24] yet implemented Google Buzz, which was the subject of a recent settlement with the FTC. These examples demonstrate that unregulated self-application of FIPPs by entities with financial or security interests contrary to privacy will apply them in surprising, incongruent, or even shocking ways.

NSTIC should mandate that all Identity Ecosystem marketplace Participants comply with FIPPs. Regulations should be developed under two guiding principles: 1. FIPPs must be implemented to protect Users' privacy interests, rather than the financial or security interests of the other Participants, and 2. FIPPs must be implemented in a contextual manner, based upon the role of each participant. Failure to do so will likely result in FIPPs having a limited influence on the Market's behavior.

Data Usage Policies will Favor IdPs or Relying Parties, Not Users' Privacy

The Data Usage Policy between the User and IdP is the foundation of all Users' privacy in an unregulated Identity Ecosystem Marketplace. An NSTIC Data Usage Policy will be a hybrid of a traditional contract, a privacy policy, probably communicated in formats that echo P3P.[25] If the Data Usage Policy is written in the User's privacy interests, then his identity will not be traded in the Identity Marketplace. But if the Data Usage Policy is vague or written by the Identity Provider, the User should expect his identity to be shared with Relying Parties, Third Parties and Attribute Providers.

Every assertion by officials that NSTIC will improve privacy relies upon one of three assumptions: 1. The Data Usage Policy will protect the User; 2. The User can create a functional substitute for privacy by fragmenting personal information across multiple Identity Providers; or 3. The Identity Ecosystem Marketplace is regulated to protect Users' privacy.

We do not think that any of these assumptions are warranted at this point, or even likely to occur. In an unregulated Identity Ecosystem Marketplace, the Data Usage Policy is the Achilles Heel of privacy. Without regulation, Data Usage Policies will be analogous to today's corporate privacy policies. Because individuals lack equal bargaining power with service providers, and despite efforts like P3P, Users must accept today's corporate privacy policies as a condition of service. Users are unable to negotiate Privacy Policies, but must accept them if they wish to receive service.

Without policy to moderate existing market forces, Identity Ecosystem Marketplace Users will have to adopt a standard Data Usage Policy written by the IdP. Users will be no more able to negotiate a Data Usage Policy in the Identity Ecosystem Marketplace than they may negotiate a Privacy Policy now.

Further, it is not difficult to imagine a scenario where, as a condition of service, a Relying Party requires a User to accept a particular Identity Provider and Data Usage Policy. Like Privacy Policies of today, those Data Usage policies will allow the IdP and Relying Party carte-blanche permission to utilize User personal information in any manner which will maximize profit.

The unequal bargaining power between a User and Identity Provider eliminates a core pillar of privacy protection within the Identity Ecosystem Marketplace. Unambiguous regulations are necessary to implement the vision and aspirations of NSTIC, so that the Identity Ecosystem mitigates, rather than exacerbates the poor privacy practices of today.

---

[21] Information on DHS Privacy may be found at http://www.dhs.gov/privacy (Accessed March 28, 2011).

[22] DHS, *Privacy Policy Guidance Memorandum*, December 29, 2008. http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf (Accessed March 28, 2011).

[23] DHS, *Privacy Impact Assessment for TSA Whole Body Imaging*, October 17, 2008, p. 5. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_wbi.pdf (Accessed March 28, 2011). *See also*, DHS, *Privacy Impact Assessment Update for TSA Advanced Imaging Technology*, January 25, 2011. http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-tsa-ait.pdf (Accessed March 28, 2011).

[24] *Google Privacy Center*, http://www.google.com/intl/en/privacy/ (Accessed March 28, 2011).

[25] According to the World Wide Web Consortium (W3C)'s website, "The Platform for Privacy Preferences Project (P3P) enables Websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents. P3P user agents will allow users to be informed of site practices (in both machine- and human-readable formats) and to automate decision-making based on these practices when appropriate. Thus users need not read the privacy policies at every site they visit." *See* http://www.w3.org/P3P/ (Accessed March 28, 2011). The project was never widely deployed and has been largely abandoned.

Identity Providers will Create Centralized Databases of Personal and Transaction Information

The IdP is a steward of vast amounts of User and transactional information. IdPs are the information center of the Identity Ecosystem. In an unregulated Identity Ecosystem Marketplace, IdPs will amass a large amount of User information, including inter-organization transactional history and personal information attributes. This information will have huge economic value, and without strict Policy safeguards, each IdP will be under strong economic pressures to collect, mine, re-purpose, sell, and share the information with the highest bidder—often the very parties from whom Users are trying to keep it.

Retail vs. Wholesale Privacy

In an unregulated Identity Ecosystem Marketplace, end-node Identity Ecosystem Participants (such as Relying Parties) may not be able to piece together a User's inter-transactional history, but each IdP will. When personal information exchange is limited between a User and Relying Party, it increases retail privacy. But once the personal information enters the Identity Ecosystem Marketplace, it may be traded among third parties, which decreases wholesale privacy. NSTIC appropriately identifies the need to limit secondary uses of attributes and preserve wholesale privacy.

Without policy and regulation to enforce NSTIC's aspirations of privacy, the strategy may well end up encouraging the appearance of retail privacy while substantially eroding or eliminating wholesale privacy.

MIT and Google researchers Arkajit Dey and Stephen Weis have long recognized that IdPs pose risks to privacy, and have even developed technology tools to deal with those problems. Notwithstanding, NSTIC does not yet require protections identified by these researchers.

> While federated login systems like OpenID may streamline logins, they may create risks to user privacy. The core problem in both centralized and federated login systems is that all user logins to Relying Party web sites must flow through an identity provider. A user's identity provider can easily link together the various websites that the user visits. An identity provider could, for example, release data about which sites users visited without user consent.
>
> ...Besides simply revealing which sites a user visits, identity providers often reveal personal information about users....[26]

In this way, NSTIC could hurt privacy by giving users a false sense of retail privacy, while facilitating the opaque trade of personal information and eliminating wholesale privacy. While this currently happens on a regular basis, NSTIC could exacerbate this problem by improving the ease and efficiency of sharing unregulated personal information.

Identity Provider's Effect on Anonymity

NSTIC envisions that a blogger will be able to "the Identity Ecosystem will preserve online anonymity and pseudonymity, including anonymous browsing."[27] NSTIC's visions of privacy and anonymity require the use of zero-knowledge proof technology. Although such technology exists, additional incentives may be required to encourage IdPs to implement zero-knowledge proofs and encourage Relying Parties to utilize IdPs who adopt this technology. Without these protections in place, as Lee Tien correctly observes, "The proposal mistakenly conflates trusting a third party to not reveal your identity with actual anonymity – where third parties don't know your identity."[28]

Without strictly enforcing zero-knowledge proofs, Identity Ecosystem "anonymity" could become nothing more than de-identification. As AOL[29] and Netflix,[30] have both learned by unfortunate trial and error, these are not synonymous concepts.

Assertions of guaranteed NSTIC privacy and anonymity are unsupportable at this point, because

---

[26] Arkajit Dey and Stephen Weis, *PseudoID: Enhancing Privacy for Federated Login*, p. 1. http://www.pseudoid.net/static/pseudoid.pdf Accessed March 28, 2011.

[27] *National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy*, April 15, 2011, p. 2. http://www.nist.gov/nstic.

[28] *Real ID Online? New Federal Online Identity Plan Raises Privacy and Free Speech Concerns*, July 20, 2010. http://www.eff.org/deeplinks/2010/07/real-id-online-new-federal-online-identity-plan (Accessed March 28, 2011).

[29] *See* http://en.wikipedia.org/wiki/AOL_search_data_scandal (Accessed March 28, 2011).

[30] *See* http://en.wikipedia.org/wiki/Differential_privacy#Netflix_Prize, and http://en.wikipedia.org/wiki/Netflix#.22Recommendation_Algorithm.22. *See also*, Arvind Narayanan and Vitaly Shmatikov, *Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset)*, February 5, 2008. http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf (Accessed March 28, 2011).

they rest upon the assumption that Users will have unlimited bargaining power, and that Market Participants will act against their own financial interests in the altruistic pursuit of User privacy, even without regulation.

Identity Provider Databases

NIST recently released a consumer-targeted video that asserts all NSTIC federated identity systems will require Identity Providers to be blind to Users' online activities: "Your ID Provider would not know how you use your credential," the video says, "There is no central database tracking your actions."[31] These statements are simply not supportable by NSTIC, which provides aspirational guidance, but no requirements at this point.

Future NSTIC implementation documents must prevent Identity Providers from tracking Users' online behavior. For the reasons explained above, Identity Providers have the means and incentives to track online User behavior.

Unfortunately, the video also uses the term "centralized database" ambiguously. On one hand, it is true that NSTIC will not create a single government-owned database which tracks all online User behavior. On the other hand, without regulation to prevent aggregation, IdPs will have the means and incentives to create their own centralized tracking databases, which they could aggregate with other centralized databases from Attribute Providers and other IdPs, to create larger centralized databases.

Using Multiple IdPs to Achieve Data Fragmentation

Technologists counter that a single User can create a functional substitute for privacy by managing multiple identities for different activities. Indeed, a National Academies study, *Who Goes There?: Authentication Through the Lens of Privacy*,[32] found that multiple, separate, and truly unlinkable credentials improve security and privacy. Though maintaining multiple identities is technologically feasible, the argument is illusory for at least four reasons.

First, managing multiple identities is inconvenient. It is well established that Users are not able to manage more than a few credentials such as usernames and passwords, or even credit cards. In theory, carrying credit cards from dozens or hundreds of independent credit card companies might prevent a single company from having easy access to a User's entire transactional history. But most people carry one or two cards, just as most people are likely to have just one or two IdPs.

Second, the Identity Ecosystem Marketplace must be regulated to place limits on the amount of information an IdP can collect about an individual. For example, let's say that a User utilizes a particular IdP to make a verified claim that she is over 13 years old, and for no other reason. Even though the IdP may only need her date of birth, unregulated IdPs may collect and store an unlimited amount of personal information about her from other IdPs and Attribute Providers, for marketing or business reasons. And unfortunately that additional information would likely be outside the scope of the Terms of Service, nor subject to the Data Usage Policy. In essence, this means that any privacy protection provided by the Data Usage Policy would apply only to the date of birth, but not to any other information collected by the IdP.

Third, the argument is illusory because unregulated IdPs may aggregate fragmented databases, especially when multiple IdPs are owned by the same parent company. As Lee Tien points out,[33] the problem of linking identities under a single Umbrella Identity has yet to be addressed. We hope that the academic work of Stefan Brands,[34] or Jan Camenisch[35] and Anna Lysyanskaya[36] on this subject will be implemented in mandatory technical standards. Otherwise, unregulated IdPs may increase the perception of retail privacy, while having the perverse effect of eliminating wholesale privacy behind the scenes.

Fourth, NSTIC expresses hope that IdPs will delete personal information after a period of time, or after the User's contract with the IdP ends. However, without regulation encouraging this behavior, IdPs will be under substantial market pressures to keep, mine,

[31] "NSTIC Animated Video" at 1:27, http://www.nist.gov/nstic/animation.html hosted at YouTube, http://www.youtube.com/watch?v=ATbQnT0MSIM&feature=player_embedded#at=87, Accessed March 28, 2011.

[32] pp. 125-132. *See* http://www.nap.edu/catalog.php?record_id=10656 (Accessed March 28, 2011).

[33] *Real ID Online? New Federal Online Identity Plan Raises Privacy and Free Speech Concerns*, July 20th, 2011. http://www.eff.org/deeplinks/2010/07/real-id-online-new-federal-online-identity-plan (Accessed March 28, 2011).

[34] *See* http://www.credentica.com/the_mit_pressbook.html

[35] *See* http://www.zurich.ibm.com/~jca/publications.html

[36] *See* http://www.cs.brown.edu/~anna/research.html

enrich, and sell former Users' personal information. Instead of improving privacy, having multiple unregulated IdPs may have a detrimental effect on privacy by authorizing multiple IdPs to collect and store User personal information indefinitely.

IdPs as Identity Reporting Agencies

Once the IdP market stabilizes, a few IdPs will probably control a large segment of the Identity Provider market. While providing retail privacy to consumers, they will also amass huge warehouses of individual transactional data which dwarf Transunion, Equifax, and Experian in sheer volume and data richness. This information will have huge economic value, and IdPs could easily use this information to create an alternative to today's Credit Score. Without applying proper Policy protections like the Fair Credit Reporting Act, IdPs are poised to become Identity Reporting Agencies of tomorrow, replacing the role of today's Credit Reporting Agencies.

Identity Providers Must Be Regulated

The NSTIC model assumes that the IdP and Relying Parties will either be separate, disinterested entities, or subject to limitations on secondary use of personal information. Roles which are truly separated by corporate entity and business interests would give Identity Providers more latitude to align their business models with the interests of their Users. However, as an unregulated NSTIC Identity Ecosystem Marketplace matures, Relying Parties and Identity Providers will find economic incentives for affiliating, or becoming children of the same parent company, as illustrated in the figures herein.

Once the Relying Party and Identity Provider are related or affiliated, the Relying Party and Identity Provider will have the power to set the terms of the Data Usage Policy. As discussed earlier, IdP-mandated Data Usage Policies will undermine a core premise of NSTIC privacy. Future NSTIC implementation policy must not permit a Relying Party to require Users to utilize only affiliated Identity Providers, which may not protect User privacy.

IdPs Not Required to be Identity Oracles

Bob Blakely makes a reasonable case that "Identity Oracles" would have more incentives to keep personal information safe. Bob Blakely defines an "Identity Oracle" as,

> An organization which derives all of its profit from collection & use of your private information… And therefore treats your information as an asset… And therefore protects your information by answering questions (i.e. providing meta-identity information) based on your information without disclosing your information… Thus keeping both the Relying Party and you happy, while making money.[37]

Although we take issue with some of Bob Blakely's more nuanced conclusions, we generally agree that organizations which fit the description of an Identity Oracle will have more incentives to protect User information.

The Ideal Federated Identity transaction (see **Figures 8** and **9**) conceptualizes the Identity Provider much like Bob Blakely's Identity Oracle. However, this perception is not warranted at this point. NSTIC does not require IdPs to be Identity Oracles, or even independent organizations. Any company may also be its own Identity Provider, affiliate with an IdP, or create an IdP subsidiary. As non-Identity Oracle entities, IdPs will be subject to the same market pressures to share and monetize personal information as Relying Parties. As demonstrated in this report, these Market forces are insufficient to incentivize IdPs to protect personal information, without regulation.

Accreditation's Effect on IdP Behavior

NSTIC envisions that IdPs will be subject to an accreditation process by an independent authority. In theory, the incentive to maintain a trustmark granted by an accreditation authority should positively mitigate market forces and improve the IdP's behavior.

While we encourage an independent accreditation process and support the concept of a meaningful trustmark, there is no guarantee that the yet-unwritten accreditation requirements will affect IdP behavior or improve User privacy. Further, there are no shortage of popular accreditations and trustmarks on the market today designed to instill confidence in online eCommerce (e.g., Hackersafe, Verisign, TrustE, PCI-DSS, PayPal, ISIS, etc.). It remains to be seen whether yet another trustmark will instill more trust among Users, and more importantly, whether the trust is warranted.

---

[37] See Bob Blakley's 2006 presentation on the subject at http://podcast.burtongroup.com/ip/2006/06/identity_and_co.html, and an informative follow-up blog post here: http://identityblog.burtongroup.com/bgidps/2007/10/what-the-identi.html

User Rights will End Upon Data Policy Deletion

In general, two parties who end a contract have no further responsibility to one another, absent a fiduciary duty, legal responsibility, or unless a contract clause survives termination. The Data Usage Policy is a contract between the User and IdP. Given the unequal bargaining power between the two parties, one should expect that in an unregulated Identity Ecosystem Marketplace most Data Usage Policies will favor the financial interests of the IdP over the privacy interests of the User, especially upon termination.

Higher-value transactions necessitate commensurate policy, procedural, and technology safeguards to minimize abuse of identity credentials.

Terminating this relationship presents unique challenges. NSTIC recognizes the need to allow Users to timely delete personal information, which would bind future data stewards. Without regulatory protection to this end, the Data Usage Policy may not require deletion after contract termination. Unless the contract is written to protect the User's privacy interests, the IdP's contractual duties to not share personal information would end at the termination of the contract, as illustrated in **Figure 19**.

Limiting secondary use after the termination of the Data Usage Policy is essential to meet Users' expectations, because they will be induced to share personal information with IdPs, under the promise of contractual protection.

Identity Credentials will be Analogous to an Internet "Power of Attorney" Without Procedural Safeguards

A "Power of Attorney" is a legal instrument which empowers a person to act on someone else's behalf in a legal or business matter. A person with a Power of Attorney can create contracts on another's behalf, or even make life-or-death decisions should the person become incapacitated. These are powerful legal instruments, and state laws impose strict procedural safeguards such as signing, witnessing and notarizing, to ensure that a power of attorney is not fraudulently obtained or abused. As a result, it is exceedingly difficult or impossible to create a Power of Attorney by accident or mistake.

An NSTIC credential is designed to be a trusted internet identification which will permit Users to fill prescriptions, purchase real estate, access financial accounts, and enter contracts. If NSTIC is successful at creating a truly "trusted" identity online, then NSTIC credentials will be extremely powerful.

Transferring a powerful NSTIC credential to a spouse or other trusted party will be a convenient way to authorize that person to act on a User's behalf. In fact, a transferred NSTIC credential will create more than an agent relationship, it will allow a person to assume another's identity.

This issue is more than theoretical. In fact, earlier this week, the Virginia legislature, with support from the Smart Card community, passed a law allowing a signed digital identity to be used in lieu of notarization.[38]

NSTIC must develop a vocabulary to discuss this issue. To introduce the subject, we analogize a powerful NSTIC credential to an Internet Power of Attorney, because of the range of transactions it enables. NSTIC does not yet propose a framework for identifying when or how an NSTIC credential may be used as an Internet Power of Attorney. However, one thing is clear: Online, as in real life, higher-value transactions necessitate commensurate policy, procedural, and technology safeguards to minimize abuse of identity credentials.

NSTIC implementation plans and regulation must explore whether, if ever, a service provider such as a doctor, attorney, or insurance broker should be able to demand that a User transfer his NSTIC credentials to enable the doctor to make life-saving decisions on the User's behalf; or the attorney to remotely sign documents on her client's behalf; or the insurance broker to purchase the cheapest insurance on behalf of the User.

Transferring a credential carries risk. If a User gives his root credentials to a Relying Party, then the Relying Party may enter into a relationship directly with an IdP of its choice, and take control of the identity credential on behalf of the User. If the User choses to revoke her Internet Power of Attorney with the Relying Party, she must depend upon the Relying Party to cease using the credential. Canceling the credential (or other credentials issued to the Relying Party by other IdPs, based upon the Claims of the first credential) may not be possible, if the Relying Party asserts ownership over it, or owns the IdP issuing the

[38] *Virginia law enables electronic notarization*, http://www.secureidnews.com/2011/04/13/virginia-law-enables-electronic-notarization. Accessed April 15, 2011.

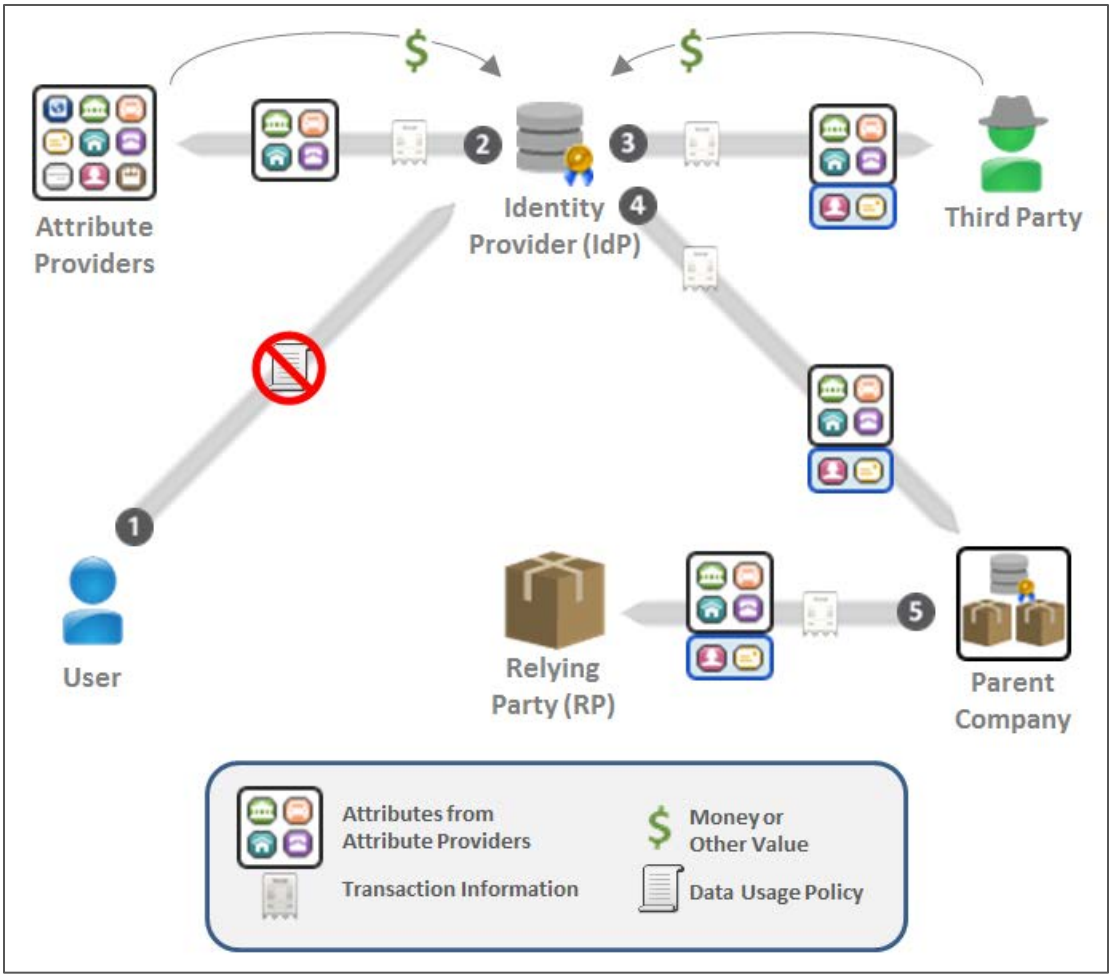

Figure 19: User Ending Relationship with IdP (Identity Market Diagram)

Ending a contract with an Identity Provider may create the following challenges:

1. The User terminates the relationship and Data Usage Policy between himself and the Identity Provider.
2. Free from contractual obligations to the User, the Identity Provider may now sell personal information enriched with Transaction Information to Attribute Providers…
3. …and Third Parties.
4. The Identity Provider may still share User information with Parent Companies.
5. Parent Companies may share it with other child companies.

credential. This would require the User to prove her identity in real life again, causing inconvenience equivalent to recovering from Identity Theft.

NSTIC must propose policy to regulate the proper use of NSTIC credentials as a *de facto* Internet Power of Attorney, and set up procedural guidelines on how to transfer or revoke the transfer, of credentials to a third party.

Currently, no single credential, including a social security card or driver license, will permit a third party to exercise the degree of control over his identity as an NSTIC credential may. This new policy vulnerability must be taken seriously by policy-makers, Users, and businesses.

NSTIC Credentials will Create New Identity Theft Vectors

The primary practical difference between a Power of Attorney and Identity Theft is a User's authorization.

Identity theft occurs when someone pretends to be a User (without authorization), does something bad, and the User gets blamed. For example, Financial Identity Theft occurs when an unauthorized individual impersonates a victim for the purpose of stealing financial assets. Medical Identity Theft occurs when someone pretends to be a victim, has a medical procedure, and disqualifies the victim from receiving medical insurance or benefits in the future. Criminal Identity Theft occurs when someone impersonates a victim, commits a crime, and the victim is charged with the crime.

Currently, many forms of Identity Theft rely upon the Social Security Number. It took decades for the American public to learn the sensitivity of the SSN, and without proper training from the outset, the public may not understand that an NSTIC credential should be protected even more vigilantly than a social security card.

Some NSTIC credentials will be extremely powerful, and if placed on a portable identity medium such as a smart card or cell phone, will fall into the hands of unauthorized individuals on a regular basis when the media is lost or stolen.

An NSTIC credential will enable forms of hyper-identity theft. In addition, without proper regulations, a powerful and highly-trusted NSTIC credential may be used by an unauthorized individual to create new NSTIC credentials with other IdPs, which may be less powerful and trusted, but still valuable to the attacker. NSTIC must address the case where a trusted Identity Medium is stolen and used to authorize new, independent credentials from other IdPs which would allow an attacker to secretly utilize the User's identity even after the original credential is revoked.

The Federal Government has begun a public relations campaign in which they assure the public that NSTIC is safe, secure, and private. Indeed, the aspirations of NSTIC are exactly as the officials describe. But assurances of privacy and security are unwarranted and unsupportable at this point. We hope that the public relations campaign will mention the importance of keeping an NSTIC Identity Medium more private than a social security card.

We fear that in the coming 5-10 years we will see a world of Identity Theft beyond the SSN, where an individual's identity credentials may be high-jacked and used against him with much more devastating consequences. And we fear that without the proper messaging from the outset, the public will not protect their identity credentials as they should. And by the time we re-learn the lessons of the social security number, we will have lost tens of millions more victims to Identity Theft and other related crimes.

Unregulated Relying Parties May Use NSTIC IDs to Over-Identify Users

Many online forums, newspapers and blogs have begun to discourage or prohibit completely anonymous commenting on their websites, forcing Users to register with an email address, for example. Service providers understand that website usage drops by nearly a factor of 10 for each additional piece of personal information requested from Users because of the time and effort Users must expend to share the data. Thus, service providers have a market incentive to ask for the minimum amount of personal information necessary.

With an easy-to-use NSTIC credential, service providers may be able to demand more information about Users' identities than before, because of the ease of divulging the information. Users may not fully appreciate that swiping their smart card or clicking "yes" when prompted, may authorize the service provider to fully identify the person, even if the identity is not posted online.

NSTIC recognizes the need to minimize over-identification, but we do not believe that self-regulation will sufficiently protect privacy among all Identity Providers. The risk of over-identification increases whenever easy identification is available.

Steven Bellovin, Professor of Computer Science at Columbia University, noted this risk in NSTIC when he wrote, "We need ways to discourage collection of identity information unless identity is actually needed to deliver the requested service."[39]

Currently, over-identification is costly and inefficient. NSTIC will enable a cheap, easy, and opaque method to over-identify Users.

NSTIC Must Provide Recourse to Correct False Information or Damage to Reputation

Victims of Identity Theft find that the most difficult part of recovering is removing false and damaging information from their credit histories. Given the potential risk for abuse of NSTIC credentials, we are disappointed that the policy does not recognize the need for legislation to help individuals recover from NSTIC Identity Theft. Issues of governance remain an unresolved issue.

Several privacy bills are currently making their way through Congress, and we hope that NSTIC implementation policy will create clear guidance to lawmakers on privacy protections necessary within the context of NSTIC.

NSTIC May be Similar to, but is Not a "National ID"

Several commentators have expressed skepticism to downright disdain for NSTIC as a back-door approach to instituting a National ID.[40] Instituting any sort of national identification can have serious and unanticipated consequences, and should be the subject of a robust public policy debate. However, based upon our analysis of NSTIC, **NSTIC itself is not an identification system, much less a National ID**. NSTIC is a framework for setting up a structure of interoperable federated identity systems. Each system will be owned and operated by various independent private companies and public institutions, using various technologies with various levels of identity assurance, security, and trust levels.

We decline to call NSTIC a "National ID." Instead, we think it is much more prudent to discuss attributes which may be similar or dissimilar to a centralized, federal-government-issued National ID card. We hope that the following table can focus the public discussion on this matter, which is currently lacking articulation.

How NSTIC is Not Like a National ID	How NSTIC Might be Like a National ID
NSTIC credentials are not owned, issued, or managed by the Federal Government, except for IDs issued to government employees.	If adopted by a majority of state governments, NSTIC credentials could become standard in State IDs and drivers licenses. The Federal Government could also embed an NSTIC credential in passports.
Identity Provider Databases are not under government control, except for a few run by the Federal Government for government employees.	Identity and personal information which enters the Identity Ecosystem Marketplace is subject to very little protection against government search and seizure under the 4th Amendment.
NSTIC is voluntary for the private sector and private citizens.	If adopted by State governments, which control a substantial portion of the identification market, NSTIC credentials could become mandatory and displace private sector identity competitors.
NSTIC credentials are not yet required to access government benefits.	Access to electronic government services may one day require an NSTIC credential.

We acknowledge that if NSTIC is widely adopted by the private and public sectors, it may also be adopted by state governments and embedded on state ID cards, for example. This scenario could create a state-by-

[39] Steven Bellovin, *Comments on the National Strategy for Trusted Identities in Cyberspace*, July 12, 2010. http://www.circleid.com/posts/comments_on_the_national_strategy_for_trusted_identities_in_cyberspace/ (Accessed March 28, 2011).

[40] *See, e.g.*, Lee Tien and Seth Schoen, *Real ID Online? New Federal Online Identity Plan Raises Privacy and Free Speech Concerns*, July 20th, 2010. http://www.eff.org/deeplinks/2010/07/real-id-online-new-federal-online-identity-plan (Accessed March 28, 2011). *See also*, *Obama Eyeing Internet ID for Americans*, January 7, 2011. http://www.cbsnews.com/8301-501465_162-20027837-501465.html (Accessed March 28, 201). *See also*, JD Rucker, *Why Obama's National Internet ID Solution is a Really, REALLY Bad Idea*, January 10, 2011. http://www.techi.com/2011/01/obamas-national-internet-id/ (Accessed March 28, 2011).

state structure of interoperable identity systems, which could theoretically behave much like a National Identification system. Though the concern that NSTIC will become a platform for a National ID is not completely unfounded, we believe that the argument is exaggerated, plagued with ambiguity, and distracts from other policy flaws that create more inevitable dangers to U.S. citizens' privacy.

We agree with the Center for Democracy and Technology's Jim Dempsey who said,

> The Obama Administration is not planning to create a government ID for the Internet. In fact, the Administration is proposing just the opposite: to rely on the private sector to develop identities... for online commerce.... [T]he government needs an identity ecosystem or identity infrastructure. It needs it for its own services as well as part of the solution to the broader Cybersecurity problem as well as one of the foundations of eCommerce, but the government cannot create that identity infrastructure. Because if it tried to, it wouldn't be trusted.[41]

[41] Jim Dempsey, *New Urban Myth: The Internet ID Scare*, January 11, 2011. http://www.cdt.org/blogs/jim-dempsey/new-urban-myth-internet-id-scare (Accessed March 28, 2011).

Conclusion and Recommendations

If implemented correctly, a national framework of interoperable federated identity systems could promote security, and trusted identities, while enhancing privacy. Identity Finder supports any effort that will help individuals control their personal information, improve privacy and security, and decrease the use of the social security number as a primary identifier.

NSTIC aspires to be privacy-enhancing, but success is far from assured. To the contrary, several Market forces, combined with NSTIC's shyness to recommend regulations that would ensure privacy, mean that NSTIC's vision has a long, steep road ahead if it is ever to become reality.

To date, official messaging has painted NSTIC as inevitably privacy-enhancing. While Identity Finder shares NSTIC's vision of privacy, we are concerned that it is too early to declare victory. We hope that future messaging will acknowledge that major hurdles to these goals remain unresolved, and that NSTIC is not a no-risk venture.

The NSTIC strategy might set a ceiling, rather than a floor, for privacy protections.

Recommended Policy Enhancements

Based upon the analysis in this document, we have identified a long list of unresolved policy hurdles that NSTIC must address before it will be capable of protecting privacy in the way it envisions. Among these policy requirements are:

- All Identity Ecosystem Participants must be held to technical and legal standards which implement FIPPs, baseline privacy and security protocols.
- Participants should be prohibited from sharing personally identifiable information without consent, even to parent companies or affiliates.
- Successful implementation of the Ecosystem should not create incentives to commoditize human identity.
- NSTIC must find ways to compensate for Users' lack of bargaining power with IdPs.
- NSTIC must preserve "retail" and "wholesale" privacy.
- NSTIC must regulate IdPs' foreseeable role as the "Identity Reporting Agency" of the future; subject to laws similar to the Fair Credit Reporting Act.
- NSTIC must create default rules protecting Users' privacy expectations upon deletion of the Data Usage Policy.
- The Data Usage Policy should apply to all information an IdP possesses about a User from all sources, not just User-provided Attributes.
- NSTIC must create a framework for discussing how and when it is appropriate to transfer NSTIC credentials to trusted third parties (such as a spouse, attorney, doctor, etc.) to use as a type of Internet Power of Attorney.
- NSTIC must create clear rules on over-identification.
- Public messaging regarding NSTIC should begin to train Users now, on the importance of safeguarding their Identity Media.
- NSTIC should create procedural mechanisms to recover from identity theft and abuse of NSTIC credentials.
- NSTIC should apply standards to existing IdPs such as Facebook, Google, and Twitter.
- Users must have the legal right to permanently delete personal attributes from the Identity Ecosystem.
- Consumers and advocates must have a meaningful voice in the ongoing development of NSTIC policy.
- NSTIC policy should prohibit Relying Parties from requiring Users to utilize only affiliated or owned IdPs.
- Regulations must ensure that secondary uses of personal information are extremely limited.
- Regulations must ensure that any personal information must be stored in a secure manner.
- NSTIC should require the implementation of zero-knowledge proofs before an Identity Provider is permitted to claim that its services are "Anonymous," instead of simply de-identified.
- NSTIC must develop legal theories that would create a legal relationship between Users and Attribute Providers which allows the User to restrict how the Attribute Provider shares Attributes with third parties, even if the Attribute Provider derived the Attribute.

- Most, if not all, of these rules and policies should be given the full force and effect of law.

Without Regulation, NSTIC will be Unable to Protect Privacy

The last decade has seen the unprecedented commoditization of human identity. We fear that the NSTIC strategy might set a ceiling, rather than a floor, for privacy protections. Absent regulation, we are concerned that NSTIC will fall far short of implanting its vision of a privacy-protecting Identity Ecosystem.

This report concludes that the exchange of data and money through a typical federated identity transaction creates multiple market incentives to use technology that will increase profits at the expense of privacy. An unregulated Identity Ecosystem will open new markets for commoditizing human identities, and absent policy to the contrary, will create new security risk vectors for individuals who participate in an NSTIC federated identity system.

To counteract these market forces, NSTIC policy should contain unambiguous and mandatory restrictions on how NSTIC participants may use sensitive personal information, based upon well-accepted Fair Information Practice Principles (FIPPs). Although NSTIC envisions an Identity Ecosystem of FIPPs and privacy, it has not yet envisioned the need for regulation to make its aspirations a reality.

Meeting NSTIC Requirements

NIST officials insist that NSTIC is voluntary, privacy-enhancing, secure, resilient, cost-effective, and easy to use. Any Participant who fail to meet these principles is in violation of NSTIC. We applaud NSTIC's vision of a safe, secure, and private Identity Ecosystem.

We are anxious, however, that NSTIC does not set the necessary tone for development necessary to make NSTIC's aspirations a reality, and may set a ceiling on privacy protections. We are also concerned that the public messaging surrounding NSTIC is unwarrantedly rosy, and fails to acknowledge the substantial privacy, security, and market hurdles that remain to be solved. If implemented within a mature regulatory framework, NSTIC could drastically improve privacy, security and online trust. But it is too early to claim victory.

The NIST official was mostly right in at least one respect—many of the potential abuses described in this paper are already happening without the knowledge or consent of Users. What remains to be seen is whether NSTIC's influence on the markets will translate from aspiration to regulation. Without regulation, NSTIC could end up exacerbating the existing market failures and severely cripple online privacy.

The stakes are high. A hammer may be used for construction or demolition. Should NSTIC be implemented without the benefit of regulation, the same tools that could be used to enhance privacy could instead be used to undermine or eliminate it. NSTIC articulates a vision where all technological tools are used constructively to preserve privacy; we now hope that the implementation document includes calls for regulation so that privacy tools are used as intended—to enhance privacy.

About Identity Finder

Identity Finder, LLC (Velosecure, LLC), was founded in 2001 by innovative security experts and is headquartered in New York City. Its technology gives users the ability to find and protect sensitive data. In addition to outstanding technology, Identity Finder prides itself on producing quality thought leadership on issues of privacy, security, and identity. The management team is comprised of globally recognized specialists that are thought leaders in the security and privacy industry.

The company has quickly grown to become a leader in data loss prevention and identity theft prevention by helping millions of consumers, small businesses, and enterprises in over fifty countries. The Identity Finder Series is the company's flagship line of data leakage prevention products. Using the company's proprietary AnyFind technology, Identity Finder intelligently and automatically locates social security numbers, credit card numbers, bank accounts, passwords, driver's licenses, dates of birth, and other private data that can be used to commit identity fraud. The product searches within files, emails, browsers and other system areas where people might not even realize their computer stored their details. Beyond identification, the technology helps securely shred or encrypt information. The Identity Finder DLP Suite is ideally suited for small to large organizations, while the Free, Home Edition and Premium Editions are designed for individual users.

Identity Finder's ultimate goal is to work ourselves out of business by encouraging responsible use and storage of sensitive personal information.

About The Authors

Aaron Titus, Esq.: Principal Author

The lead author if this report, Aaron Titus is currently the Vice President of Business Development and Chief Privacy Officer for Identity Finder, and an attorney specializing in Internet, Technology and Privacy law. Aaron has spent four years as the Privacy Fellow for the Washington DC policy institute Liberty Coalition. There he helped develop Privacy Commons: An emerging framework for creating complete, informative, enforceable, and easy to adopt privacy policies. He also developed NationalIDWatch.org, empowering individuals to recover from identity breach and theft.

As an attorney he has consulted organizations on legal requirements, risk identification, risk management, and developing a corporate culture of privacy. In May 2010 he testified before the Senate Committee on Homeland Security and Government Affairs. Aaron Titus received his J.D. from the George Washington School of Law, and his undergraduate degree in Architecture from the University of Utah.

Aaron Titus' work has been covered in countless newspapers and news media outlets, including the Washington Post, New York Times, Forbes, the Wall Street Journal, The Associated Press, ABC, MSNBC, (and NPR's *Wait Wait Don't Tell Me*). He is an Eagle Scout and proud husband and father of five small under the age of five.

Mr. Titus is a member of a broad range of working groups, policy organizations, and privacy standards development organizations, including the Privacy Coalition, several Kantara Privacy working groups, the Identity Commons Stewards Working Group, and others. Mr. Titus has been a leading voice in the national discussion about the impacts of NSTIC on Privacy.

Todd Feinman: Editor

In 2001, Todd co-founded Identity Finder, LLC. Since then he has taken the role of CEO and transformed Identity Finder into a leader in security and privacy helping consumers prevent identity theft and businesses prevent data leakage. Todd is an internationally published author and media personality. He wrote Microsoft's own reference book on securing Windows and McGraw Hill's university textbook on managing the risks of electronic commerce. Over the past fifteen years, he has appeared on CBS, ABC, FOX, NBC, FOXNews, and has

presented at numerous global conferences on the topics of security and privacy.

Todd spent ten years at PricewaterhouseCoopers, where he started as an ethical hacker breaking through the IT security of Fortune 100 companies and later took the role of Director where he led and grew the integration services group of their security and privacy consulting practice. Todd also worked as a product manager for Microsoft in their .Net server group.

Todd has a Master in Business Administration from Harvard Business School and a Bachelors of Science from Lehigh University.

David Goldman: Editor

David is a co-founder of Identity Finder, LLC with overall responsibility for operations and product management. Leveraging his deep expertise in information security and a decade of client-focused experience as a Director with PricewaterhouseCoopers, David also works closely with customers to develop new solutions. He has written numerous white papers and articles and has presented at industry conferences and international symposia. David has a Bachelor of Science in Computer Science from Washington University in St. Louis.

Copyright and Creative Commons License Notice

The purpose of this report is to enrich the public discussion and encourage debate. The authors hope that academics, technologists, policy makers, the public, and the media will reuse, republish, and remix the contents of this report with attribution to Identity Finder and the Authors.

[42] Identity Finder, LLC's website is http://www.identityfinder.com

[43] The Creative Commons Attribution 3.0 Unported License may be found at, http://creativecommons.org/licenses/by/3.0/

Appendix A: Public Discourse on NSTIC to Date

Most recently with an event at Stanford University,[44] development of a PSA-style video on NSTIC,[45] and the recent release of the NSTIC strategy document, federal government officials have begun to push NSTIC out of the realm of geeks and technologists into the mainstream media. In general, public discussion about NSTIC has fallen into six categories. Articles exemplifying each of these major points are referenced here as background information. These categories are:

- General Analysis of NSTIC
- Benefits of NSTIC
- NSTIC as a Back-Door National ID
- NSTIC Feasibility
- NSTIC's Effect on Privacy and Civil Liberties
- Reporting on Department of Commerce's Administration of NSTIC

General Analysis of NSTIC

Alex Howard did an excellent job at summarizing the implications and importance of NSTIC in his article, *2011 Trends: National Strategy for Trusted Identities in Cyberspace highlights key online privacy, security challenges*.[46] Rick Merritt also wrote an overview piece on NSTIC for the EE Times.[47]

Benefits of NSTIC

Businessweek's James Sterngold ran a series on how NSTIC will reduce or eliminate the ubiquitous username and password as a means of accessing online resources.[48] Omar El Akkad of the Globe and Mail outlined the need for trusted identities online and benefits like using a single credential for multiple online resources.[49]

NSTIC as a Back-Door National ID

The Electronic Frontier Foundation's (EFF) Lee Tien and Seth Schoen outlined why NSTIC could easily turn into a *de facto* National ID, with serious consequences for privacy, security, and liberties.[50] A CNET and CBS News story discussed the possibility of NSTIC as a government-issued "Internet ID for Americans."[51] JD Rucker of techi.com expressed deep skepticism about a "National Internet ID's" effect on privacy, security, behavioral monitoring, and other related issues.[52]

In reply, identity expert Kaliya Hamlin wrote an Op Ed for Fast Company entitled "...Why We Shouldn't Freak Out About NSTIC."[53] She reminds readers of the myriad problems Users face on the internet without a trust layer and says, "No one I have ever talked to in government wants [to create a National ID]".

While expressing cautious skepticism about some of NSTIC's policies, Jim Dempsey of the Center for Democracy and Technology underlined his support for NSTIC and rejected the claim that it was a government

---

[44] Video and transcripts of the Forum on NSTIC at Stanford University, January 7, 2011, are available at http://www.nist.gov/nstic/video.html (Accessed March 28, 2011).

[45] PSA-style video available at http://www.nist.gov/nstic/animation.html or http://www.youtube.com/watch?v=ATbQnT0MSIM (Accessed March 28, 2011).

[46] January 7, 2011. http://gov20.govfresh.com/2011-trends-national-strategy-for-trusted-identities-in-cyberspace-highlights-key-online-privacy-security-challenges/ (Accessed March 28, 2011).

[47] *White House ramps up secure ID program*, January 7, 2011. http://eetimes.com/electronics-news/4212003/White-House-ramps-up-secure-ID-program (Accessed March 28, 2011).

[48] *Internet Identity System Said Readied by Obama Administration*, January 07, 2011. http://www.businessweek.com/news/2011-01-07/internet-identity-system-said-readied-by-obama-administration.html (Accessed March 28, 2011). See also, *Say Goodbye to All Those Passwords*, January 27, 2011. http://www.businessweek.com/magazine/content/11_06/b4214036537462.htm (Accessed March 28, 2011).

[49] *U.S. eyes Internet user ID system*, January 10, 2011. http://www.theglobeandmail.com/news/technology/tech-news/us-eyes-internet-user-id-system/article1864855/ (Accessed March 28, 2011).

[50] *Real ID Online? New Federal Online Identity Plan Raises Privacy and Free Speech Concerns*, July 20th, 2010. http://www.eff.org/deeplinks/2010/07/real-id-online-new-federal-online-identity-plan (Accessed March 28, 2011).

[51] *Obama Eyeing Internet ID for Americans*, January 7, 2011. http://www.cbsnews.com/8301-501465_162-20027837-501465.html (Accessed March 28, 201).

[52] *Why Obama's National Internet ID Solution is a Really, REALLY Bad Idea*, January 10, 2011. http://www.techi.com/2011/01/obamas-national-internet-id/ (Accessed March 28, 2011).

[53] *National! Identity! Cyberspace! Why We Shouldn't Freak Out About NSTIC*, January 10, 2011. http://www.fastcompany.com/1715659/national-identity-cyberspace-why-we-shouldnt-freak-out-about-nstic (Accessed March 28, 2011).

attempt to nationalize citizens' identity,[54] echoing a report by *Wired's* Ryan Singel that the strategy's implementation rests squarely on the shoulders of the private sector. [55]

NSTIC Feasibility

Don Thibeau of Open ID Foundation (OIDF) takes no position on NSTIC but indicates that it is collaborating with the NSTIC team in developing trust frameworks for "industry self regulation and market expansion."[56] Michael Hickins of the Wall Street Journal interviewed a cautiously optimistic Bruce Schneider on the technological feasibility of NSTIC.[57] And Steven Bellovin, Professor of Computer Science at Columbia University, expressed skepticism that NSTIC would be viable in the market, or preserve privacy. [58]

NSTIC's Effect on Privacy and Civil Liberties

The NSTIC home page at nist.gov unambiguously asserts that NSTIC protects Users privacy, "This new 'identity ecosystem' protects your privacy. Credentials share only the amount of personal information necessary for the transaction. You control what personal information is released, and can ensure that your data is not centralized among service providers."[59] A January 7, 2011 Department of Commerce press release asserts that NSTIC is "...aimed at establishing identity solutions and privacy-enhancing technologies that will make the online environment more secure and convenient for consumers." [60] *The Hill* quotes White House Cybersecurity Coordinator Howard Schmidt as saying, "NSTIC plans to nurture the development of a secure and privacy-enhancing 'identity ecosystem' for the Internet... This identity ecosystem would instill greater confidence in online transactions with less personal information being collected and stored with each transaction, lowering the risk of identity theft."[61]

In addition to EFF's Lee Tien and Seth Schoen, the ACLU's Jay Stanley believes that NSTIC will likely eviscerate privacy and online anonymity, not improve security, and either be too expensive or under-developed when launched.[62] Joe Campana's three-part series warns that NSTIC could facilitate Identity Theft, and that online identity may have unintended consequences on offline life and liberty. [63]

Reporting on Department of Commerce's Administration of NSTIC

A number of reports have announced the existence of NSTIC and the Department of Commerce's role in developing the strategy. These include, *PC World*,[64] *InformationWeek*,[65] *Pulse2.com*,[66] *Fedscoop.com*,[67] *Dark Reading*,[68] and *The Hill*.[69]

---

[54] *New Urban Myth: The Internet ID Scare*, January 11, 2011. http://www.cdt.org/blogs/jim-dempsey/new-urban-myth-internet-id-scare (Accessed March 28, 2011).

[55] *Obama's Solution for Online ID? Let Silicon Valley Take the Lead*, January 7, 2011. http://www.wired.com/epicenter/author/ryan_singel/ (Accessed March 28, 2011).

[56] *The US "NSTIC" and the "Open Identity for Open Government" Initiative*, January 24, 2011. http://openid.net/2011/01/24/the-us-nstic-and-the-open-identity-for-open-government-initiative/ (Accessed March 28, 2011).

[57] *Cyber-Security Czar Defends Government Role*, February 15, 2011. http://blogs.wsj.com/digits/2011/02/15/cyber-security-czar-defends-government-role/ (Accessed March 28, 2011).

[58] Steven Bellovin, *Comments on the National Strategy for Trusted Identities in Cyberspace*, July 12, 2010. http://www.circleid.com/posts/comments_on_the_national_strategy_for_trusted_identities_in_cyberspace/ (Accessed March 28, 2011).

[59] *National Strategy on [sic] Trusted Identities in Cyberspace*, http://www.nist.gov/nstic/ (Accessed March 28, 2011). See also, http://www.nist.gov/nstic/animation.html (Accessed March 28, 2011)

[60] *U.S. Commerce Secretary Gary Locke, White House Cybersecurity Coordinator Howard A. Schmidt Announce Next Steps to Enhance Online Security, Planned National Office for Identity Trust Strategy*, January 7, 2011. http://www.commerce.gov/news/press-releases/2011/01/07/us-commerce-secretary-gary-locke-white-house-cybersecurity-coordinato (Accessed March 28, 2011).

[61] Gautham Nagesh, *Locke announces new office to secure online transactions*, January 9, 2011. http://thehill.com/blogs/hillicon-valley/technology/136867--locke-announces-new-office-to-secure-online-transactions (Accessed March 28, 2011).

[62] *Don't Put Your Trust in "Trusted Identities,"* January 13, 2011. http://www.huffingtonpost.com/jay-stanley/dont-put-your-trust-in-tr_b_806096.html (Accessed March 28, 2011).

[63] Examiner.com, *White House strategy for secure cyberspace based on identity-theft-flawed meatspace (part 2)*, June 29, 2010. http://www.examiner.com/x-9215-Identity-Theft-Examiner~y2010m6d29-White-House-strategy-for-secure-cyberspace-based-on-identitytheftflawed-meatspace-part-2 (Accessed March 28, 2011). *White House strategy for secure cyberspace based on identity-theft-flawed meatspace (part 3)*, July 1, 2010. http://www.examiner.com/identity-theft-in-national/white-house-strategy-for-secure-cyberspace-based-on-identity-theft-flawed-meatspace-part-3 (Accessed March 28, 2011).

[64] Grant Gross, *White House Officials Push Online Trusted IDs*, January 7, 2011. http://www.pcworld.com/businesscenter/article/216143/white_house_officials_push_online_trusted_ids.html (Accessed March 28, 2011).

[65] Nicholas Hoover, *Commerce Department To Head Web Identity Initiative*, January 10, 2011.

http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=229000404&subSection=Privacy (Accessed March 28, 2011).

[66] Amit Chowdhry, *White House Announces National Strategy for Trusted Identities in Cyberspace (NSTIC)*, June 25, 2010. http://pulse2.com/2010/06/25/white-house-announces-national-strategy-for-trusted-identities-in-cyberspace-nstic/ (Accessed March 28, 2011).

[67] Luke Fretwell, *NIST Simplifies NSTIC*, March 16, 2011. http://fedscoop.com/video-nist-simplifies-nstic/ (Accessed March 28, 2011).

[68] Tim Wilson, *White House Advances 'Trusted Identities' Program*, Jan 11, 2011. http://www.darkreading.com/authentication/167901072/security/privacy/229000437/index.html (Accessed March 28, 2011).

[69] Gautham Nagesh, *Locke announces new office to secure online transactions*, January 9, 2011. http://thehill.com/blogs/hillicon-valley/technology/136867--locke-announces-new-office-to-secure-online-transactions (Accessed March 28, 2011).


identityfinder