Oklahoma Journal of Law and Technology

Volume 11 | Number 1

January 2015

The Sky is not Falling: An Analysis of the National Strategy for Trusted Identities in Cyberspace and the Proposed Identity Ecosystem

Aaron L. Jackson
aaron.jackson@ou.edu

10 Okla. J.L. & Tech. 74 (2015)
www.okjolt.org

THE SKY IS NOT FALLING: AN ANALYSIS OF THE NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE AND THE PROPOSED IDENTITY ECOSYSTEM

© 2015 Aaron L. Jackson*

Table of Contents

* Judge Advocate General's Corps, United States Air Force. Major Jackson is currently assigned to the Washington D.C. area as an LL.M. student at The George Washington University Law School. Prior to this assignment, Major Jackson served in numerous legal positions within the United States Air Force, to include prosecutor, defense attorney, and Deputy Staff Judge Advocate. This article was provided by Major Jackson in his private capacity and does not reflect the position or opinion of the United States Air Force or the United States Government. Major Jackson would like to thank his wife (Beth) and three children (Matthew, Mackenzie, and Mary) for their love and patience as he diligently worked on this article.

I. Introduction

Cyber experts have long envisioned a day when the multiple password-based systems used for identification and authorization of individuals on the internet would be replaced with a singular, online identity.[1] That day may be coming soon. In 2011, the National Institute of Standards and Technology (NIST), the federal technology agency entrusted with development of industry standards, finalized the National Strategy for Trusted Identities in Cyberspace (NSTIC).[2] Dubbed a "driver's license" for the internet,[3] this policy envisions the creation of an Identity Ecosystem where individuals may forego their multiple password-based online identities for one secure identity used "for convenient, secure, and privacy-enhancing [internet] transactions anywhere, anytime."[4] Far beyond conceptual, two states and one federal agency

[1] *See* Colin Wood, *Are You Ready for a Driver's License for the Internet?*, GOV'T TECH. (Apr. 25, 2014), http://www.govtech.com/security/Drivers-License-for-the-Internet.html.
[2] *National Strategy for Trusted Identities in Cyberspace (NSTIC)*, ELECTRONIC PRIVACY INFO. CENTER, http://epic.org/privacy/nstic.html (last visited Oct. 29, 2014) [hereinafter *NSTIC*].
[3] Natasha Singer, *Call It Your Online Driver's License*, N.Y. TIMES, Sept. 18, 2011, at BU4, *available at* http://www.nytimes.com/2011/09/18/business/online-id-verification-plan-carries-risks.html.
[4] Naomi Lefkovitz, Nat'l Inst. of Standards & Tech., Identity in Cyberspace: Improving Trust and Overcoming Barriers via Public-Private Partnerships (n.d.) (unpublished presentation), *available at* http://apps.americanbar.org/dch/thedl.cfm?filename=/CL320041/relatedresources/03-NL-NSTIC-ABA-IdM-Mtg.pdf.

have now begun the process of turning the NSTIC's Identity Ecosystem into a reality.[5]

The NSTIC represents the classic intersection of two competing concepts: security and liberty. Those in favor of the policy cite the rise in cybercrime, crippling cost of online fraud and identity theft, and need to enhance online protections as primary motivation for the program.[6] Opponents to the NSTIC, such as the Electronic Frontier Foundation, are quick to highlight the practical and constitutional issues created by an Identity Ecosystem.[7]

This article takes the position that the NSTIC, as it currently exists, does not pierce the constitutional veil. Moreover, the practical evolution of the Identity Ecosystem will likely remain clear of the constitution as well. Opponents of the NSTIC misunderstand the current state of the policy and go too far in their predictions of the future. This position is not taken lightly, however, and emphasizes the need for enhanced legislation to defend against the legitimate concerns raised by privacy advocates. As misguided as their assessment of the NSTIC might be, the influence of the program's opponents is exactly what is needed to keep the Identity Ecosystem in proper balance.

---

[5] Tim Sampson, *Michigan and Pennsylvania Become First States to Test Universal Internet IDs*, DAILY DOT (May 6, 2014), http://www.dailydot.com/news/government-michigan-pennsylvania-test-internet-ids/; *see also* John Breeden II, *NSTIC Is Moving Forward, but Does It Even Have a Chance?*, FEDSCOOP (Sep. 18, 2014, 10:18 PM), http://fedscoop.com/will-government-password-consolidation-lead-increased-security/ (discussing development of a pilot program within the Department of Veterans Affairs).

[6] *See generally* OFFICE OF THE WHITE HOUSE, NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE (Apr. 2011) [hereinafter NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE], *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

[7] *See, e.g.*, Meghan Neal, *The White House Wants to Issue You an Online ID*, MOTHERBOARD (Apr. 28, 2014), http://motherboard.vice.com/read/the-white-house-wants-to-issue-you-an-online-id.

II. Evolution of the Identity Ecosystem

From social media to online shopping to banking, the internet provides tools for nearly every facet of daily life. As internet technology has increased, so has the rise in online participation. Between 2000 and 2014, the number of internet users across the globe increased by over 676%.[8] By 2014, approximately three billion people (39% of the world's population) used the internet worldwide.[9] The internet has become a vital tool for operating in an increasingly technological world. Americans alone spend an average of more than four hours online each day.[10] Unfortunately, with the rise in cyber technology has comes an exponential growth in cyber-related crimes. The NSTIC represents an evolution of federal policy developed over the past decade in response to this ever-increasing cyber threat. However, before one may discuss the existing state of policy, it is important to first understand its origins.

A. The 2003 National Strategy to Secure Cyberspace

To combat the rise in cyber incidents, President George W. Bush initiated the National Strategy to Secure Cyberspace in 2003.[11] As recognized by the President, "In the past few years, threats in cyberspace have risen dramatically."[12] Therefore, "improving our ability to respond to cyber incidents and reduce the potential damage from such events" represented a fundamental and ever-increasing national security concern.[13] Among several notable aspects of the National

---

[8] *Id.*
[9] *Internet Usage Statistics: The Internet Big Picture*, INTERNET WORLD STATS, http://www.internetworldstats.com/stats.htm (last visited May 5, 2015).
[10] Chip Babcock, *Let's Stop Giving the FCC Free Rein to Regulate the Internet*, FORBES (May 5, 2014, 9:59 AM), http://www.forbes.com/sites/realspin/2014/05/05/lets-stop-giving-the-fcc-free-rein-to-regulate-the-internet/.
[11] OFFICE OF THE WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE (Feb. 2003), *available at* http://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.
[12] *Id.*
[13] *Id.*

Strategy of Secure Cyberspace, the policy recognized that protecting the nation from cyber-threats required more than government involvement. "Securing cyberspace is an extraordinarily difficult strategic challenge that requires a coordinated and focused effort from our entire society – the federal government, state and local governments, the private sector, and the American people."[14] Whether President Bush realized it at the time, this announcement set the long-term stage for a public-private Identity Ecosystem on the internet.

B. Homeland Security Presidential Directive-12 (HSPD-12)

As a first-wave defense to the exploding cyber threat, President Bush focused on strengthening the electronic systems of the federal government. At the time, many of the federal agencies maintained differing security and authentication requirements for systems and personnel.[15] In addition to being asynchronous across federal agencies, employee authentication systems simply required use of a single password,[16] a security approach long identified by experts as an "inadequate" protective measure.[17] As a result of the "[w]ide variations in the quality and security of identification used to gain access to secure facilities," President Bush released Homeland Security Presidential Directive-12 in 2004.[18] Within this directive, the President ordered creation of a "Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees)."[19]

---

[14] *Id.*
[15] *See generally NSTIC*, *supra* note 2 (author also relies, in part, on his personal knowledge of inter-agency security operations).
[16] *Id.*
[17] Wood, *supra* note 1.
[18] Office of the White House, Homeland Security Presidential Directiv-12 (Aug. 27, 2004), *available at* http://www.dhs.gov/homeland-security-presidential-directive-12.
[19] *Id.*

This push for a uniform federal identification and authentication standard led to the creation of the Common Access Card (CAC).[20] The CAC remains the standard identification card used by federal employees throughout the government today.[21] Roughly the size of a credit card, the CAC includes multiple external employee identifiers such as the picture, name, rank (if applicable), service/agency, and specific affiliation of the specific federal employee.[22] In addition to more commonly used identifiers, the CAC possesses "smart card" technology through an embedded microchip (with encryption technology), magnetic strip, and barcode that store data unique to each user.[23] As a result, this single card provides access to secure locations in the physical and cyber domains across the spectrum of federal agencies.[24]

Utilization of the CAC, as a singular identity tool for physical and virtual environments, goes far beyond simple access to the federal computer system. As a practical example of the new identification system's benefits, consider the "Air Force Portal."[25] Air Force personnel utilize "the portal" as the primary link to many electronic systems used by service members, including military pay, military leave, emergency notification records, personnel documents, and Department of Defense email.[26] Prior to creation of the CAC, each of these systems required separate registration and authentication requirements, making operation in the Air Force cyber domain complex and cumbersome. Implementation of the CAC linked all systems to the single

---

[20] *See generally NSTIC*, *supra* note 2 (author also relies, in part, on his personal knowledge of inter-agency security operations).
[21] The author relies heavily on his personal experience as a federal employee when discussing federal agency security technology and use of the CAC system.
[22] *Common Access Card (CAC) Security*, DoD CAC, http://www.cac.mil/common-access-card/cac-security (last visited Oct. 29, 2014).
[23] *Id.*
[24] *See supra* note 21.
[25] *See supra* note 21.
[26] *See supra* note 21.

authentication tool. Rather than maintain numerous separate accounts, access to all network sites now required a simple, two-step authentication process: 1) physical insertion of the CAC into a digital reader and 2) a unique PIN code specifically linked to the CAC.[27] The impact of these cybersecurity changes was clear. Not only did this new authentication system drastically increase efficiency and operability,[28] "DoD [Department of Defense] network intrusions fell 46% after it banned passwords for log-on and instead mandated use of the CAC. . . ."[29] As a result of its successes using the CAC card, the NSTIC highlights the DoD as an entity "leading the way" to further implementation of enhanced authentication technology.[30]

C. National Security Presidential Directive-54 (NSPD-54)

Presumably resulting from the success of previous efforts at the federal level, President Bush implemented National Security Presidential Directive-54 (NSPD-54) in January 2008.[31] Focused on protecting our nation's public and private infrastructure, NSPD-54 provided a vision to enhance digital identification and authentication requirements throughout the country in order to "improve the Nation's security against the full spectrum of cyber threats. . . ."[32] As noted by the President within this directive:

> Cyber criminals are intent on malicious activity, including the manipulation of stock prices, on-line extortion, and fraud. These activities cost American citizens and businesses tens of billions of dollars each year. Hackers and insiders have penetrated or shut down utilities in countries on at least three continents. Some

---

[27] *See supra* note 21.
[28] *See supra* note 21.
[29] Lefkovitz, *supra* note 4.
[30] *Id.*
[31] *See generally Senate Cybersecurity Information Sharing Bill Proposed*, ELECTRONIC PRIVACY INFO. CENTER (Jun. 20, 2014), http://epic.org/2014/06/senate-cybersecurity-informati.html. **Error! Bookmark not defined.**
[32] Office of the White House, National Security Presidential Directive-54, at 1 (Jan. 8, 2008), *available at* http://epic.org/privacy/cybersecurity/EPIC-FOIA-NSPD54.pdf.

> terrorist groups have established sophisticated on-line presences and may be developing cyber attacks against the United States.[33]

Unlike HSPD-12, which focused on securing the federal system, this initiative appeared to take the first steps toward expanding its security policy into the private sector. Additionally, as noted by the Electronic Privacy Information Center (EPIC), this directive reveals "the government's long-standing interest in enlisting private sector companies to monitor user activity."[34]

D. The 2009 Cyberspace Policy Review

After the election of President Barak Obama, the White House returned once more to its cyber policy, publishing the *Cyberspace Policy Review* on May 29, 2009.[35] Designed as a "60-day, comprehensive, 'clean-slate' review to assess U.S. policies and structures for cybersecurity,"[36] President Obama provided the following vision:

> The Federal government - in collaboration with industry and the civil liberties and privacy communities - should build a cyber-security-based identity management vision and strategy for the Nation that considers an array of approaches, including privacy-enhancing technologies. The Federal government must interact with citizens through myriad information, services, and benefit programs and thus has an interest in the protection of the public's private information as well.[37]

While couched as a simple review process, the Cyberspace Policy Review, in its verbiage, seems to advocate and build upon previous White House efforts to create a more secure online environment for all Americans. One privacy organization defines the Cyberspace Policy

---

[33] *Id.* at 2.
[34] *Senate Cybersecurity Information Sharing Bill Proposed*, *supra* note 31.
[35] OFFICE OF THE WHITE HOUSE, CYBERSPACE POLICY REVIEW (May 29, 2009), available at https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf [hereinafter CYBERSPACE POLICY REVIEW]..
[36] *Id.* at iii.
[37] *Id*. at 33.

Review as creating a "national plan for a public secure Internet identification program."[38] While taking a bold move toward greater online security for all Americans, President Obama correctly identified the conflict between privacy and security that provides the foundational issue within this article. In advocating concern for the latter, the President makes his position clear: "People cannot value security without first understanding how much is at risk."[39] This continued push for enhanced internet security led to the creation of the NSTIC.

E. The National Strategy for Trusted Identities in Cyberspace (NSTIC)

Two years after conducting the Cyberspace Policy Review, experts within the White House finalized the NSTIC.[40] This document serves as the implementation tool for the goals identified within the 2009 Cyberspace Policy Review[41] and envisions an online environment where "[i]ndividuals and organizations utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation."[42] Achievement of this vision comes through "the user-centric **'Identity Ecosystem,'** an online environment where individuals and organizations are able to trust each other because they follow agreed upon standards to obtain and authenticate their digital identities—and the digital identities of devices."[43] In other words, as noted by one columnist, "standard password protection is dead,"[44] replaced with a more robust authentication system.

---

[38] *NSTIC*, *supra* note 2.
[39] CYBERSPACE POLICY REVIEW, *supra* note 35, at iv.
[40] *See NSTIC*, *supra* note 2.
[41] Breeden, *supra* note 5.
[42] NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE, *supra* note 6.
[43] *About NSTIC*, NAT'L INST. OF STANDARDS & TECH., http://www.nist.gov/nstic/about-nstic.html (last visited Oct. 29, 2014).
[44] Breeden, *supra* note 5.

In developing the Identity Ecosystem, the NSTIC "consists of the participants, policies, processes, and technologies required for trusted *identification, authentication,* and *authorization* across diverse transaction types."[45] Successful implementation of the ecosystem concept may enhance the security of a wide array of internet exchanges, from banking to networking, by aiding in the ability of both participants to accurately identify the individual or entity on the other end of the exchange. Conceptualizing the Identity Ecosystem may be difficult. As a result, the NSTIC offers the following practical example:

> …[i]ndividuals or NPEs [non-person entities] acting within the Identity Ecosystem can obtain a pseudonymous or uniquely identified credential from an identity provider before conducting transactions online. For higher levels of assurance, identity providers validate subjects' physical identities and make sure that each digital identity accurately reflects the actual person or NPE. Next, identity providers associate a subject's credential with the subject's digital identity. . . . A subject obtains a validated attribute claim to use in online transactions. . . . . [T]he individual or NPE presents credentials and attributes directly to the relying party. The subject uses privacy-enhancing technologies to minimize the information that is revealed to the relying party. The relying party can then validate the credentials and attributes without the need for the identity or attribute providers to know that the subject is performing the transaction. . . . Relying parties are able to authenticate that the credentials and attributes are from valid providers and are current. A subject supplies validated credentials and attribute claims to a relying party to authorize an online transaction. Likewise, an individual or NPE is able to make informed choices about relying parties by checking whether or not the relying party has a "trustmark," which certifies that it adheres to the rules of the Identity Ecosystem. When the individual accesses the online services of the relying party, the trustmark is electronically validated.[46]

The Identity Ecosystem will not rely on government sources to maintain identity and authentication databases. Rather, the NSTIC envisions use of public-private partnerships.[47] In January 2011, Commerce Secretary Gary Locke announced that the NIST "would be responsible for the digital identity framework;" however, "implementation would be outsourced to the

---

[45] NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE, *supra* note 6.
[46] *Id.*
[47] *Id.*

private market, eliminating the need for a central database."[48] As one columnist writes, "In other words, private businesses, like Target, will get a shot at protecting our now singular online identities."[49]

Private companies offering secure authentication technology is not a new idea. In July 2008, Facebook unveiled its "Connect" concept, which offered "third-party websites tools to coordinate with the user information that Facebook holds, including logins."[50] As a result, "websites had the option of allowing Facebook users to identify themselves with their Facebook identities."[51] The government may look to other companies, such as Google and PayPal, to provide the necessary technology as well.[52] As early as 2008, a conglomerate of companies including AT&T, Google, PayPal, Symantec and Verizon created the "Open Identity Exchange," a concept designed to "develop certification standards for online identity authentication."[53] Other companies like ApplePay and the Smart Card Alliance also appear eager to participate.[54]

Since its development in 2011, the NSTIC has transitioned from the theoretical to the practical. In the fall of 2013, the NIST awarded a total of $2.4 million in grants to Minnesota and Pennsylvania for implementation of the first pilot programs.[55] As of the summer of 2014,

---

[48] *NSTIC*, *supra* note 2.
[49] David Anderson, *Internet Driver's License*, RICHFIELD REAPER (Jun. 11, 2014, 8:00 AM), http://www.richfieldreaper.com/opinion/columnists/columnist_one/article_c59c3898-db7f-11e3-967f-0019bb2963f4.html.
[50] Simson Garfinkel, *Facebook Wants to Supply Your Internet Driver's License*, MIT TECH. REV. (Jan. 5, 2011), http://www.technologyreview.com/news/422285/facebook-wants-to-supply-your-internet-drivers-license/.
[51] *Id.*
[52] Singer, *supra* note 3.
[53] *Id.*
[54] *See* Breeden, *supra* note 5; *see also* Smart Card Alliance Endorses the NSTIC Framework, SMART CARD ALLIANCE, http://www.smartcardalliance.org/publications-smart-card-alliance-endorses-the-nstic-framework/ (last visited Oct. 29, 2014).
[55] Wood, s*upra* note 1.

these programs were underway.[56] Rather than create entirely new authentication systems out of whole cloth "or even some form of comprehensive Internet wide identification system, the implementations in each state look at how existing systems can be used to simplify authentication across departments."[57] For the moment, these programs appear focused on creating authentication systems for users working with government agencies at the state and local levels.[58] Specifically, Pennsylvania is "developing an implementation that would allow users to operate a single identity across state departments, rather than requiring users to manage usernames and passwords for each department, which is the case today."[59]

In addition to state-based initiatives, the federal government launched its own pilot program with the Department of Veterans Affairs.[60] Similar to the existing authentication currently used by companies such as PayPal,[61] the federal ecosystem looks to establish an identification and authentication system for citizen interaction with the federal government through a singular website known as Connect.gov.[62] Though unclear at this point, this website may offer a singular point of entry for access to various federal agencies similar to the Air Force Portal concept discussed above. Depending on its success, additional federal agencies may

[56] *See, e.g.*, Sampson, *supra* note 5.
[57] Wood, *supra* note 1.
[58] *See generally id.*
[59] *Id.*
[60] *See* Breeden, *supra* note 5.
[61] See *generally id.*
[62] *See* Aliya Sternstein, *Exclusive: New Connect.Gov Aims to Consolidate Your Passwords*, NEXTGOV (Sep. 15, 2014), http://www.nextgov.com/cybersecurity/2014/09/new-connectgov-aims-consolidate-your-passwords/94154.

join.[63] Development of the Identity Ecosystem remains in its infancy stage; however, a fully developed online ecosystem may emerge as early as 2020.[64]

Despite the program's current focus on government-based systems, the transition to e-commerce and other private markets will certainly follow. As envisioned by the NSTIC, "Imagine a world where individuals can conduct sensitive business transactions online with reduced fear of identity theft or fraud and without the need to manage scores of usernames and passwords."[65] The transition strategy provided by the NSTIC makes clear its wide-reaching intent by providing the following series of goals: 1) develop and strengthen the Identity Ecosystem; 2) implement the ecosystem at the local/state/federal levels; 3) enhance consumer confidence in the Identity Ecosystem through "education and awareness" measures, thereby promoting "widespread adoption of the Identity Ecosystem" in the United States; and finally 4) ensure "long-term success" of the program with an eye toward "integrat[ing] the Identity Ecosystem internationally."[66] As noted by the NSTIC, "The greater number of participants in the Identity Ecosystem, the greater the value that each will obtain from participation."[67]

It is important to emphasize that the NSTIC calls for purely volunteer participation.[68] Much of the implementation strategy focuses, not on compelling cooperation, but educating the populace regarding the benefits of participating in a secure Identity Ecosystem.[69] However, despite the seemingly innocuous development of the NSTIC, its implications are, as stated within

---

[63] *See* Breeden, *supra* note 5.
[64] *Id.*
[65] NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE, *supra* note 6.
[66] *Id.*
[67] *Id.* (citing the third goal of the NSTIC).
[68] *Id*. (stating that the first of the NSTIC's "guiding principles" is to ensure that "[i]dentity solutions will be privacy-enhancing and voluntary").
[69] *See id*.

the NSTIC, "widespread."[70] It is clear that the NSTIC seeks nothing less than to revolutionize the internet. If the NSTIC achieves is goals, "it could pave the way for an interoperable authentication protocol that works for any website, from your Facebook account to your health insurance company."[71] And yet, surprisingly, its implementation has received little public attention. Rather than remain in the dark, the remainder of this article sheds light on this important topic, focusing next on the "pros" and "cons" of the NSTIC.

III. The Pros

The online environment represents a virtually endless road of opportunity, innovation, and advancement. However, despite the plethora of positive attributes associated with the internet, challenges have emerged in the decades of electronic advancement. The internet has saved and ruined lives. Many have pushed for greater internet control, a reining in of the worldwide web for the overall benefit of mankind.[72] This section seeks to identify and discuss the primary advantages of the NSTIC.

A. Reduction in Cyber Crime

There is no doubt: cybercrime is big business. As of 2006, the Federal Bureau of Investigation estimated that cybercrime cost United States businesses $67.2 billion.[73] Average costs per company reached approximately $24 thousand.[74] Examples of the pervasiveness of cybercrime may be seen at the local level as well. For example, of 1600 Miami businesses

---

[70] *Id.*
[71] Neal, *supra* note 7.
[72] See generally Ryan Singel, *Desperate Botnet Battlers Call for an Internet Driver's License,* WIRED (Jun. 4, 2007), http://archive.wired.com/politics/security/news/2007/06/bot_strategy.
[73] Joris Evers, *Computer Crime Costs $67 Billion, FBI Says*, CNET NEWS (Jan. 19, 2006, 2:20 PM), http://news.cnet.com/Computer-crime-costs-67-billion,-FBI-says/2100-7349_3-6028946.html.
[74] *Id.*

visited by federal agents in 2007 "that had billed for 'durable medical equipment' . . . 481 . . . didn't even exist, accounting for $237 million of fraud in just one year."[75] A quarter of a billion dollars, in one city, in a single year. And this only represents health care fraud.

Not only does cybercrime have devastating effect on businesses but individuals as well. As of 2004, according to a Javelin Strategy & Research study, identity fraud cost American citizens $52.6 billion.[76] According to cybersecurity firm McAffee, "37,413 new malicious programs hit the internet last year, including exploit code and bots."[77] This equates to development and release of one new computer virus roughly every fifteen minutes. As a result, citizens and businesses alike face the enormous challenge of protecting their electronic systems from cyber-attacks on a minute-by-minute basis. Such invasions can result in devastating loss to both person and purse.

As noted in its policy declaration, combating cybercrime lies at the heart of the NSTIC:

> The Nation faces a host of increasingly sophisticated threats to the personal, sensitive, financial, and confidential information of organizations and individuals. Fraudulent transactions within the banking, retail, and other sectors–along with online intrusions into the Nation's critical infrastructure, such as electric utilities–are all too common. As more commercial and government services become available online, the amount of sensitive information transmitted over the Internet will increase. Consequently, the probability of loss associated with data theft, unauthorized modifications, fraud, and privacy breaches will also increase. Although the total amount of losses–both financial and non-financial–due to online fraud and cybercrime is difficult to quantify, the problem is real and it is increasing.[78]

---

[75] Wood, *supra* note 1.
[76] Evers, *supra* note 73.
[77] Singel, *supra* note 72.
[78] NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE, *supra* note 6 (citing *2009 Internet Crime Report*, INTERNET CRIME COMPLAINT CENTER (IC3) (Mar. 12, 2010), http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf.)

The NSTIC approaches this threat head-on by pushing implementation of a more secure internet environment through the Identity Ecosystem. Providing internet users a more secure option that utilizes enhanced security and authentication technology when operating in the cyber realm has the potential to significantly decrease the staggering statistics associated with cybercrime. The possible benefits are not merely hypothetical; entities that currently use such enhanced security techniques have seen a marked decrease in cyber-attacks. On the federal side, as noted above, enhanced security within the Department of Defense resulted in a 46% decrease in network intrusions.[79] In the private sector, PayPal's robust authentication requirements, "using the handoff type password technology proposed by the NSTIC," have resulted in greater security without, to the author's knowledge, ever suffering from a mass-data hack.[80]

As internet technology becomes more sophisticated, so do the criminals. Cyber-attacks and cyber-crime increase each year, with little response to the mounting threat. Technology requirements proposed by the NSTIC have the ability to drastically deter cybercrime, making our nation's citizens, businesses, and infrastructure more secure.

B. Economic Gain

Providing a secure option for online data exchanges, both public and private, has the potential to reduce government expenditures and enhance overall economic prosperity. Turning first to the public domain, on-line authentication systems significantly decrease the administrative cost of providing government services to its citizens. In Florida, for example, the Department of Children and Families implemented a robust on-line authentication tool that cost

[79] Lefkovitz, *supra* note 4.
[80] Breeden, *supra* note 5.

taxpayers $3 million.[81] This electronic program allowed for greater on-line exchange, thereby reducing overall personnel demands and saving taxpayers $14.7 million.[82] "The DCF says the technology is saving so much money because it saves staff the time of verifying identities manually, and even better, there's been a reduction in cases of identity fraud."[83] Implementation of like programs across the government spectrum could significantly decrease overall government expenditures, potentially saving taxpayers billions of dollars while simultaneously reducing incidents of fraud.

Economic benefits are not limited to government cost savings. Enhanced authentication and security requirements online have the potential to significantly increase profitability of companies engaged in e-commerce. Providing citizens and businesses with an option to operate in a more secure online environment benefits both sides of the exchange. The Identity Ecosystem allows a consumer to identify the business as an authenticated entity, while the company may identify the individual on the other end of the exchange as a legitimate consumer. This level of security increases the visibility of the exchange while reducing fraud at both ends, thus yielding an increased trust in online purchasing and greater participation in the e-commerce realm. More easily put, "If people have a simple, easy way to prove who they are online with more than a flimsy password, they'll naturally do more business on the web."[84]

[81] Wood, *supra* note 1.
[82] *Id.*
[83] *Id.*
[84] Singer, *supra* note 3.

According to one senior policy advisor, retail sales online are projected to reach $2 trillion in 2016.[85] Enhanced consumer trust during online exchanges could result in a $500 billion increase to total sales.[86] Regardless of whether these figures provide accurate commercial predictions, the study provides statistical support to an obvious conclusion: trust matters when it comes to online transactions.[87]

Finally, reduction in online fraud and other cyber-related crime stimulates the economy. Even a marginal decrease in cybercrime due to enhanced security and authentication requirements proposed by the NSTIC would potentially save billions of dollars each year for private consumers and public businesses. This additional stimulus, which would have otherwise been lost to crime, could promote further consumer activity and allow businesses to further invest in infrastructure, enhance services, and/or reduce consumer prices. Securing the online environment has potential to save significant taxpayer dollars while providing economic security, stability, and prosperity.

C. Convenience and Efficiency

Nobody likes waiting in line at the DMV.[88] It is a dreaded trip citizens make each year, and it is just one example of the often time-consuming and frustrating trips made by individuals to local, state, and federal agencies. As one columnist writes, "What if states had a better way to authenticate your identity online, so that you didn't have to make a trip to the DMV?"[89]

---

[85] Lefkovitz, *supra* note 4 (citing *Rethinking Personal Data: Strengthening Trust*, WORLD ECON. FORUM (May 2012), http://www.weforum.org/reports/rethinking-personal-data-strengthening-trust).
[86] *Id.*
[87] *Id.*
[88] See Singer, *supra* note 3.
[89] *Id.*

Enhanced identification and authentication technology reduces the need for many of these dreaded experiences.

Members of the Armed Forces enjoy the convenience and efficiency of enhanced identity and authentication technology utilized by the Department of Defense. Prior to implementation of the CAC card, as previously detailed above, exchanges within the online federal system were often time-consuming and cumbersome. The myriad systems utilized by the federal government tended to overwhelm incoming personnel. Access to military pay, military leave, personnel records, emergency locator data, and physical fitness reporting (just to name a few) each required separate user names and passwords. This often led to either forgotten information (which required the additional time of re-creating verification data) or a laundry list user names and passwords written on a hidden sheet of paper (which created a significant security risk). Moreover, lack of enhanced security resulted in frequent breaches, yielding loss of private data.

The introduction of the CAC system eliminated much of these concerns. Now, the verification and authentication data imbedded within the CAC card provides a singular source for access to all online systems. Rather than create individual user names and passwords, the system merely requires insertion of the CAC card, with imbedded authentication, and a singular user password. Moreover, the differing systems are now interoperable, leading to more fluid and secure online operation.

While the NSTIC design does not propose a physical identification card such as the CAC, nor will such a system likely result from the NSTIC, a singular online identity for operations within the Identity Ecosystem does provide a level of convenience currently unknown to citizens. Not only would a similar system save significant time on-line, enhanced identity and authentication technology likely eliminates the need for travel to business or government

agencies for identification verification. Trips that once took half a day may now be accomplished in minutes from the comfort of one's home – thus alleviating the headache that often comes with a trip to the DMV.

IV. The Cons

Despite the benefits that may come with the Identity Ecosystem, one cannot ignore the many legal and practical challenges presented by this program. Of the little discussion currently devoted to this issue, the large majority appears to stand in opposition to the NSTIC, fervently declaring the beginning to the end of freedom on the internet. While the program remains in its infancy, one need not look too far into the future nor strain their imagination too great to understand the potential concerns underlying this program. This section provides a basic understanding of the negative aspects of the NSTIC.

A. Privacy

Ironically, the NSTIC sites "privacy" as among the first of its guiding principles.[90] But this internal declaration has not fooled privacy advocates. Opponents to the NSTIC fiercely assert that creating a singular online identity destroys rather than protects privacy.[91] The Electronic Frontier Foundation labels the proposed Identity Ecosystem as "radical" and an "unprecedented threat . . . to privacy . . . online."[92]

Neither the United States Constitution nor the Bill of Rights specifically mentions a right to privacy. This legal concept remained virtually unspoken for over a century after our nation's

---

[90] *See* NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE, *supra* note 6.
[91] Singer, *supra* note 3.
[92] Tim Cushing, *US Government Begins Rollout of Its "Driver's License for the Internet"*, TECHDIRT (May 5, 2014, 9:57 AM), https://www.techdirt.com/articles/20140503/04264427106/us-government-begins-rollout-its-drivers-license-internet.shtml.

inception until a young Louis Brandeis crafted an argument for constitutional privacy in 1890.[93] Some twenty-six years before attaining the status of Supreme Court Justice, Mr. Brandeis most simply referred to the idea as "the right to be let alone."[94] Since that time, the doctrine has emerged at various moments in our nation's legal history.

The Supreme Court's initial discussion of a citizen's general right to privacy emerged with the rise in technology as it related to criminal law and procedure.[95] As observed by the Court, "Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet."[96] Even prior to declaring a constitutional right to privacy, the Court continued to assert a certain level of privacy within the criminal realm.[97] Since that time, privacy rights have been repeatedly asserted by the Court in this area of law.[98] However, the Court's declared

---

[93] *See* Samuel Warren & Louis Brandeis, Note, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); *see also* Tim Sharp, *Right to Privacy: Constitutional Rights & Privacy Laws*, LIVE SCI. (Jun. 12, 2013, 5:34 PM), http://www.livescience.com/37398-right-to-privacy.html.

[94] Warren & Brandeis, *supra* note 93, at 193.

[95] Olmstead v. United States, 277 U.S. 438 (1928) (regarding law enforcement's investigatory use of warrantless wiretapping).

[96] *Id.* at 474 (upholding the use of warrantless wiretapping). Despite the privacy concerns rising from the development of technology, the Court's precedent in *Olmstead* remained intact for nearly forty years until its reversal in *Katz v. United States*, 389 U.S. 347 (1967).

[97] In *Mapp v. Ohio*, for example, the Court declared that

> without [the exclusionary rule], the freedom from state invasions of privacy would be so ephemeral and so neatly severed from its conceptual nexus with the freedom from all brutish means of coercing evidence as not to merit this Court's high regard as a freedom 'implicit in the concept of ordered liberty.

367 U.S. 643, 655 (1961).

[98] The Court continues to assert its *Katz* analysis today. As recently recognized by the Court, "Our later cases have applied the analysis of Justice Harlan's concurrence in that case, which said that a violation occurs when government officers violate a person's 'reasonable expectation of privacy.'" United States v. Jones, 132 S. Ct. 945, 950 (2012) (citing *Katz*, 389 U.S. at 360).

constitutional right to privacy was not forged from criminal procedure, but rather, marital law.[99] Over the decades since *Griswold*, additional rights to privacy have been added to the list.[100] As a result, though not specifically enumerated or universally declared, the Supreme Court continues to assert and expand upon an individual's right to privacy. How this right extends to the internet, however, remains undefined.

On a practical level, some technology experts "foresee challenges in instituting across-the-board privacy protections for consumers and companies."[101] For example, a singular, authenticated identity streamlines tracking and data collection of the user, allowing "trusted" companies within the Identity Ecosystem to amass and share data regarding every aspect of one's online behavior.[102] Interoperability requirements of systems linked to the ecosystem create further privacy concern. Stated by one critic:

> [P]eople may not want the banks they might use as their authenticators to know which government sites they visit. . . . Banks, meanwhile, may not want their rivals to have access to data profiles about their clients. But both situations could arise if identity authenticators assigned each user with an individual name, number, e-mail address or code, allowing companies to follow people around the Web and amass detailed profiles on their transactions.[103]

As Lillie Coney, associate director of the Electronic Privacy Information Center, bluntly puts it, "Look at it this way: You can have one key that opens every lock for everything you

---

[99] *See* Griswold v. Connecticut, 381 U.S. 479 (1965) (identifying a constitutional right to privacy within "the prenumbra" of the constitution, thus yielding a state's ban on contraceptives an unconstitutional restriction of a citizen's right to marital privacy).
[100] *See, e.g.*, Roe v. Wade, 410 U.S. 113 (1973) (asserting a right to privacy in the context of abortion), *see also* Lawrence v. Texas, 539 U.S. 558 (2003) (striking down Texas anti-sodomy law).
[101] Singer, *supra* note 3.
[102] *See id.*
[103] *Id.*

might need online in your daily life [Identity Ecosystem] . . . [o]r, would you rather have a key ring that would allow you to open some things but not others?"[104]

Despite NSTIC's attempts at ensuring privacy, the program cannot avoid the perception of enhanced online monitoring at the hands of the federal government. The timing of the program's roll-out alone generates concern. As noted by one columnist, "At a time when Americans are more reticent to trust the government with their online information than ever before, officials are finally moving forward with plans for a universal online ID."[105] Continued disclosure of federal action through notorious whistleblower Edward Snowden simply creates an ominous feel to this program and enhances concerns for what the future of the Identity Ecosystem may bring. As a result, perhaps the best argument on behalf of privacy advocates is less defined. Rather than focus on specific practical or theoretical concerns, the opposition may be best suited to emphasize the perceived intrusion of the federal government into their daily lives on the internet. An individual who once enjoyed the freedom to move within cyberspace uninhibited by governmental restraint may feel their world slipping away. To some, this extent of federal control may feel closer to government intrusion than regulation. Thus, privacy advocates may be compelled to harken a return of Justice Brandeis's original argument for a citizen's constitutional right to privacy: when it comes to the internet, just leave me alone.[106]

---

[104] *Id.*
[105] Sampson, *supra* note 5.
[106] *See* Warren & Brandeis, *supra* note 93.

B. Freedom of Speech

One the most fundamental guarantees of liberty within our nation is the freedom of speech. It is first in our Bill of Rights; it represents who we are as a nation of free people.[107] As Justice Brandeis eloquently stated in *Whitney v. California* regarding the value of free expression:

> Those who won our independence believed that the final end of the State was to make men free to develop their faculties . . . . They believed that freedom to think as you will and to speak as you think are means indispensable to the discovery and spread of political truth; that without free speech and assembly discussion would be futile; that with them, discussion affords ordinarily adequate protection against the dissemination of noxious doctrine; that the greatest menace to freedom is an inert people; that public discussion is a political duty; and that this should be a fundamental principle of the American government.[108]

One of the greatest attributes of the internet is the ability to exchange information and share differing viewpoints with others. A vast amount of this internet expression is political in nature. Such communication is vital to the health of our nation, providing a certain additional "check" within our political system. As a result, the internet has for decades been a primary means of upholding this "fundamental principle of American government."[109]

Due to the nature of some speech, particularly that speech which encourages "discovery and spread of political truth,"[110] individuals may prefer expression be done in private and with the benefit of anonymity. People often feel emboldened to speak loudly and in truth when it is

---

[107] U.S. CONST. amend. I ("Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press, or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.")
[108] Whitney v. California, 274 U.S. 357, 375 (1927).
[109] *Id.*
[110] *Id.*

done in the shadows. Anonymous expression is implicit within the context of free speech.[111] Previous attempts by government actors to "unmask" those who have chosen to anonymously speak out have been swiftly shot down by the Supreme Court[112] primarily based upon the recognition that "identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance."[113]

Among the concerns of the NSTIC is the potential chilling effect that a singular online identity would have on free and anonymous speech within the internet. A universal, online identification scheme appears to shed light on expression that the Supreme Court has demanded be left in the dark. As Justice Sotomayor noted in a recent case involving the rise in GPS technology, "Awareness that the Government may be watching chills associational and expressive freedoms."[114] Although the Court in *Jones* grappled with the privacy rights of individuals as it related to use of GPS tracking systems,[115] the principle concerns apply to this setting as well.

Requiring an online identity for exchanges over the internet may be seen as one giant leap towards impermissible government oversight of private communications and conduct. In reading the NSTIC plan, it is difficult to escape the overall feeling that, to some degree, "big brother" will be watching.[116] Whether the threat is actual or, more likely, imagined does not

---

[111] The Supreme Court recognized in *Talley v. California*, 362 U.S. 60, 64 (1960), that anonymous speech has "played an important role in the progress of mankind."
[112] *See, e.g.*, NAACP v. Alabama, 357 U.S. 449 (1958); Bates v. Little Rock, 360 U.S. 516 (1960).
[113] *Talley*, 362 U.S. at 65.
[114] United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).
[115] *Jones*, 132 S. Ct. 945.
[116] *See generally* Neal, *supra* note 7.

remove the concerns associated with "chilling" the ability for people to speak their mind. Either way, there exists a real potential to stifle legitimate and important online communication.

C. Freedom of Association

For reasons similar to the freedom of speech, the NSTIC may serve to suppress the freedom of association as well. Ever since the State of Alabama attempted to compel production of private NAACP membership lists in the 1950s, the Court has recognized a constitutional right to certain private association.[117] "It is beyond debate that freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the 'liberty' assured by the Due Process Clause of the Fourteenth Amendment, which embraces freedom of speech."[118] Additionally, as the Court noted, there is a "vital relationship between freedom to associate and privacy in one's associations."[119] Failure to respect the right to *private* association, especially when that association touches on sensitive or controversial issues, may infringe upon the right. In short, open association on certain matters may result in no association at all.

Similar to the problems related to freedom of speech, a singular online identity that specifically identifies the user may infringe upon a person's right to anonymous association. Individuals who wish to remain anonymous in their online participation with certain groups may find themselves compelled to disclose their identity in order to continue their association with the group. The problem exponentially increases with the threat that one's identity may be revealed, not only to other group member, but outside entities across the internet. As with the freedom of speech, whether the eyes of "big brother"[120] are watching or not does not end the concern; any

[117] *NAACP v. Alabama*, 357 U.S. 449.
[118] *Id*. at 460-61.
[119] *Id.* at 462.
[120] *See generally* Neal, *supra* note 7.

fear created by a singular online identity that deters an individual from exercising their right to free association is also problematic.

D. Practical Problems

Beyond the constitutional issues exist a plethora of practical concerns with implementing the NSTIC. First, the singular nature of the identity is, in itself, highly problematic.[121] By providing a singular identity maintained by an external source, the NSTIC creates a single point of failure. The lack of redundancy creates a serious problem. One columnist defines this as "putting all your security eggs in one vulnerable basket." Simply put, "If a hacker gets their hands on your cyber ID, they have the keys to everything."[122]

Advocates of the NSTIC may be quick to note the success of secure systems such as PayPal and the inherent added security that would come in the creation of the identity. Note once more that PayPal has not suffered a mass hack.[123] However, one could argue that it is only a matter of time. And, with the NSTIC's approach, it would only take one time to significantly harm a user. A massive breach of an identity databank would result in full online control of any individual or company whose data has been entrusted to the particular holder. At the moment, users are able to mitigate the damage of online attacks by diversifying their identities across the internet spectrum. A breach of a single source, on the other hand, would allow virtual access to every aspect of a user's life. The damage would simply be catastrophic.

[121] *See generally* Singer, *supra* note 3; *see also* Neal, *supra* note 7.
[122] Neal, *supra* note 7.
[123] *See* Breeden, *supra* note 5.

Second, in the same vein as above, the consolidation of all aspects of an internet user's activities makes mass data an even greater threat to a user's online privacy.[124] This singular flow of information "could mean that everything said under that particular NSTIC holder's account—from 'I really like that movie' to 'I disagree with our government', with the particulars to be supplied as needed—could be traced back to one user."[125] Aside from the constitutional implications, "such a repository of useful information would not only be prime hunting ground for hackers, but corporations would pay fortunes for access to such data."[126]

Third, while the NSTIC's long-term vision includes a worldwide online security system, the short-term gain may be seen as negligible. If everyone does not participate, the security ideals proposed by NSTIC do not eliminate the problem. Cyber-criminals and identity thieves will still be able to participate outside the boundaries of the protected system, leaving those who do participate in the NSTIC vulnerable to attack.

Fourth, if full success only comes with full cooperation, the "voluntary" nature of the program may be short-lived. Perhaps this realization hits home for opponents to the NSTIC, as they may see the writing on the wall. For example, online companies who adopt the NSTIC model may eventually demand consumers also participate in order to ensure greater transparency, and less fraud, within the online exchange process. Government agencies that realize the cost savings that comes with online participation may turn to a fully automated process and eventually demand citizens' registration. As a result, individuals who would wish to

---

[124] *See* Steve Anderson, *Michigan, Pennsylvania First for "Driver's License for the Internet" Plan*, TECHZONE360 (May 6, 2014), http://www.techzone360.com/topics/techzone/articles/2014/05/06/377929-michigan-pennsylvania-first-drivers-license-the-internet-plan.htm.
[125] *Id.*
[126] *Id.*

avoid an internet identity may find themselves forced into cooperation. This implied coercion adds greater depth to the constitutional concerns discussed above.

Fifth, the NSTIC envisions privatizing storage databanks rather than keeping such sensitive information under government control.[127] While it seems Uncle Sam intends this as a means to eliminate the problematic "big brother" perception and harness private sector innovation,[128] this approach creates other concerns.[129] Public-private partnerships are commonplace in government contracting[130] and often provide synergistic effect. Advocates of the identity system may point to the user's ability within the NSTIC to "choose among multiple identity providers and digital credentials" as a means to enhance user control.[131] However, no company is perfect, and this is not a perfect solution. "In theory, this could give a company like Google or Verizon a powerful tool for accessing user data and trusting them not to misuse it for their own gain."[132] While companies such as Google already conduct significant data-mining operations, implementation of the program would further advance this controversial practice. Moreover, the government's use of multiple trusted sources may require forced cooperation between "rival" companies, something that may prove difficult.[133] While government oversight would undoubtedly exist, the NSTIC provides private companies with an even greater amount of autonomy over our daily lives.

While an authenticated online identity provides numerous benefits, the challenges are loud and clear. Creation of a singular online identity provides a face to those who would choose

---

[127] NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE, *supra* note 6.
[128] *Id.*
[129] *See generally* Sampson, *supra* note 5.
[130] *See generally* Lefkovitz, *supra* note 4.
[131] *Id.*
[132] Sampson, *supra* note 5.
[133] Breeden, *supra* note 5.

to remain anonymous, creating constitutional concerns in the areas of privacy, speech, and association. Moreover, the practical challenges with implementing such a robust online identity system are additionally troublesome, leading one to wonder whether bang is worth the buck.

V. An Argument *For* the NSTIC

Though the lines have clearly been drawn, the question is not *if* the NSTIC will emerge victorious but *when* and *to what extent*. The benefits, as proposed, are immense and mutually beneficial to businesses and citizens alike. They clearly represent a compelling governmental interest. Moreover, the ad campaign likely to be offered by the government in an effort to secure the hearts and minds of the populace is a winning one – an easy sell to an otherwise fairly indifferent online population. The challenges posed by the Identity Ecosystem are concerning and deserve attention. However, as it currently exists, the NSTIC is a constitutional program, and the practical concerns merely represent challenges to be overcome with increased effort and innovation.

A. The Reality of the Identity Ecosystem

Privacy advocates exaggerate the problems of the Identity Ecosystem, painting an overly grim picture of what the future holds that seems to conjure images of inserting a physical "Internet Driver's License" into a computer before operating on the internet highway.[134] This view is misguided and unrealistic. There will be no "driver's license,"[135] nor will there be eager government officials watching your every move on the other end of the line.

Unlike the Department of Defense's use of the CAC card, the Identity Ecosystem will likely not result in distribution of physical hardware. Rather, authentication and security

[134] *See generally* Singer, *supra* note 3.
[135] *Id.*

requirements will consist of multi-authentication prompts as suggested by some technology experts.[136] The time and expense of issuing physical "licenses" far outweighs the benefits, and requiring citizens to do so would only fuel the fire of NSTIC opponents. Implementation of the NSTIC will appear much more subtle and much less pervasive.

The NSTIC has existed in conceptual form for several years, giving its experts plenty of time to develop an appropriate strategy for long-term implementation of this program. It is clear they knew what they were doing. The NSTIC seems to have addressed the majority of concerns at the outset by creating at least the illusion that the government provides solutions to most of the program's problems. The NSTIC is still in its infancy, leaving ample time for further innovation and improvement. For now, the plan at least includes the right phraseology to mitigate the opposition's arguments.

B. Voluntary Participation

A key factor of the NSTIC is the voluntary nature of the program.[137] As designed, individuals and businesses will not be forced to participate. Rather than compelled cooperation, the NSTIC envisions a grass-roots effort where "the public and private sector will use awareness and education programs to encourage demand for the Identity Ecosystem and to inform its use."[138] Those who wish to remain non-participants will be allowed to distance themselves from the ecosystem, which, as will be discussed below, lessens the constitutional concerns that come with forced participation.

This introduces two possible paradigms for conceptualizing the Identity Ecosystem. The ecosystem is either: 1) a complete take-over or 2) a safe haven. Privacy advocates may view the

---

[136] *Id.*
[137] *See generally* Lefkovitz, *supra* note 4.
[138] NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE, *supra* note 6.

Identity Ecosystem as an attempt to forcefully take-over the entire online world. Others may view it as merely offering companies and internet users the option to engage online within a safe haven designed to enhance online security.

The appropriate way to view the Identity Ecosystem is through the latter paradigm. Build the fortress, and invite the people in. That is what the NSTIC seeks to accomplish.[139] If popularity of the ecosystem increases, the safe haven may expand to greater areas of the online world. Though it is possible that the Identity Ecosystem may eventually dominate a large spectrum of the online world, it also may not. Companies may choose to move their business within the safe haven, or they may opt to remain beyond the walls.

One problem with the expressed voluntary nature of the program, however, is the suggested coercive effect that greater participation may have on an individual wishing to refrain from joining the Identity Ecosystem. Companies that adopt enhanced identity protocol through the NSTIC may require participants to do the same, leaving some with a difficult choice: sacrifice certain amenities for the sake of remaining anonymous on the web or give up certain privacy interests in order to enjoy full online participation. This argument, however, does not remove from the equation the individual's ability to choose. They are still left with an honest decision that, although difficult, is fully theirs to make. One cannot label such a situation coercive simply based on the user's loss of certain internet amenities if they choose to remain anonymous. The fact remains: that is their choice.

These decisions are already commonplace in the technological realm. Google's voluminous user agreement, for example, includes terms and conditions that, if read and

[139] *See generally* Lefkovitz, *supra* note 4.

understood, may be considered an infringement on one's privacy.[140] Earlier this year, the internet giant "updated its terms of service to reflect that it analyzes user content including emails to provide users tailored advertising, customized search results and other features."[141] Google's efforts to scan its users' emails represent the exact concerns posed by opponents of the NSTIC. And yet, such practices have not resulted in mass consumer migration to more protected email services. In fact, Gmail exists today as "the world's largest email service."[142] It is simply the cost of doing business with Google. Those who disagree may opt to take their business elsewhere. That transitioning to a different email account may prove burdensome for people who have used the same email for years does not alter the argument. It is often difficult to change one's business and private practices. However, people commonly switch companies, such as cell phone services, when they disagree with evolving company policy. The user still maintains the power of choice: accept the company's changes or simply move on.

If successful, it is possible the Identity Ecosystem will evolve into an involuntary system. The most predictable first step toward compelled participation is in the realm of government services. Cost savings to local, state, and federal governments in rendering support to its citizens may push legislators to adopt fully online services as a means to reduce public expense. This evolution does not affect the constitutionality of the program, however, especially as it relates to government services. First, there can be no expectation of privacy when interacting with the government in areas such as filing taxes and receiving government support. A citizen's identity

---

[140] *See* John Ribeiro, *Google Updates Terms of Service to Reflect Its Scanning of Users' Emails*, PCWORLD (Apr. 14, 2014, 10:23 PM), http://www.pcworld.com/article/2143700/google-updates-terms-of-service-to-reflect-its-scanning-of-users-emails.html.
[141] *Id.*
[142] Adrian Covert, *GMail at 10: How Google Dominated E-Mail*, CNN MONEY (Apr. 1, 2014, 7:01 AM EDT), http://money.cnn.com/2014/04/01/technology/gmail/index.html.

is a vital component to the process, and proper interaction cannot take place in anonymity. Second, the minimal demands of a robust online identity when interacting with the government does not place such an added burden on the citizen to overcome the benefit to the government in added cost savings and security. Third, alternatives to online interaction will likely remain for those without computer access, leaving open to citizens an option to avoid the necessity of engaging within the Identity Ecosystem. In time, perhaps the standards will more drastically change. However, such additional changes will be measured by popular support and one's understanding of the evolving internet environment.

Market forces will ultimately drive implementation of the Identity Ecosystem. If enough people demand an alternative to the Identity Ecosystem when engaging the government or private businesses, perhaps the momentum will change. However, as noted below, that does not seem to be happening at the moment.

C. Privacy and the People

The Supreme Court has made clear that people enjoy certain rights to privacy. This paper does not attempt to minimize or quash that inherent right as a citizen. The right remains; it is real and powerful. However, defining an individual's right to privacy on the internet is difficult. The concept is amorphous and remains ill-defined. With the exception of a few cases related to criminal procedure, the extent of *internet* privacy has been largely ignored by the Supreme Court.[143] This leaves one to ponder what privacy rights exist in the internet realm. Opponents to the NSTIC who focus on inherent internet privacy rights are relying on law that simply does not exist at the moment.

[143] Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010, 2012 (2013) ("[T]he U.S. legal regime provides very little in the way of personal privacy protection, and the effect is manifest for both elites and marginalized people.").

At least one Supreme Court justice has offered a reason for the Court's silence in this area, and it involves the rapid change of technology. In *United States v. Jones*, which involved law enforcement's use of GPS technology, Justice Alito provides, "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative . . . . A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[144] In other words, leave it to the people's branch to decide where the lines should be drawn, as the Court simply cannot keep up. Law reflects societal standards. It is largely up to "the people" to define those standards.

Unfortunately for privacy advocates, "the people" currently demonstrate less interest in protecting privacy. In his 1997 article *Toward A Positive Theory of Privacy Law*, scholar Lior Strahilevitz discusses the future of privacy legislation:

> American attitudes toward privacy are highly heterogeneous, with approximately twenty-five percent of the population valuing privacy a great deal (privacy fundamentalists), twenty percent of the population not valuing their own privacy and having a difficult time understanding why anyone would care about privacy (privacy unconcerned), and the remaining fifty-five percent of the population approaching privacy in a pragmatic way that balances competing interests (privacy pragmatists). If the privacy unconcerned are indeed more disposed to participate heavily in the political process, with privacy fundamentalists tending to remain on the sidelines in political debates, the smaller group's voice in policy debates may be just as loud or even louder than the larger cohort's.[145]

While these statistics offer a solid statistical foundation, two additional factors have emerged since this article's publication that further support the overall argument. First, the rise in internet technology has likely increased the number of individuals identified as "privacy unconcerned." Behavior on social media forums suggest that the walls built around our daily lives are shrinking, voluntarily. As Pew Research reports, 74% of adult internet users participate

[144] United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring).
[145] Strahilevitz, *supra* note 143.

in social networking sites.[146] Approximately 1.23 billion people have Facebook accounts worldwide, and 556 million of those users access the website every day.[147] The world enjoys unprecedented interconnectivity at the click of a button. People share information daily – often intimate details about their lives, discussion of which may have once been considered taboo. Though unsupported by statistics, younger generations who have grown up in the internet age likely view privacy much different than older generations. This proposed evolution of privacy may increase the number of those considered "privacy unconcerned."

A recent study by the Pew Research Internet Project seems to generally confirm this hypothesis. From a survey sample 607 adults of wide-ranging ages, a large majority expressed significant concerns related to privacy on the internet.[148] Of those surveyed, 91% selected either "strongly agree" or "agree" to the statement "consumers have lost control over how personal information is collected and used by companies."[149] Of those surveyed that subscribe to social networking sites, 80% "say they are concerned about third parties like advertisers or businesses accessing the data they share on these sites."[150] Additionally, 70% express concern "about the government accessing some of the information they share on social networking sites without their knowledge."[151] While this information may suggest greater privacy concern, the more

---

[146] *Social Networking Fact Sheet*, PEW RES. CENTER: INTERNET, SCI. & TECH, http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/ (last visited Oct. 30, 2014).
[147] Jemima Kiss, *Facebook's 10th Birthday: From College Dorm to 1.23 Billion Users*, GUARDIAN (Feb. 4, 2014, 5:22 AM EST), http://www.theguardian.com/technology/2014/feb/04/facebook-10-years-mark-zuckerberg.
[148] *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RESEARCH INTERNET PROJECT, http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ (last visited Dec. 5, 2014).
[149] *Id.*
[150] *Id.*
[151] *Id.*

notable point is the lack of public response to such concerns. If the Pew survey adequately mirrors the general public's overall perception, it illustrates the point that, despite the expressed apprehension many feel when it comes to a perceived loss of online privacy, few have changed their behavior. Rather than note a decrease in participation in social networking sites and on-line activity, the market continues to expand at rapid pace. In light of this research, perhaps the more appropriate term for the "privacy unconcerned" is "privacy apathetic." Either way, the research supports the notion that internet users are more likely to respond to the Identity Ecosystem with indifference or, at most, reluctant acceptance than action.

Second, for those identified as "privacy pragmatists,"[152] the overwhelming prevalence and destruction caused by cybercrime, not to mention the convenience of the NSTIC, may result in a tendency to favor security over privacy. The benefits of enhanced protection to deter cybercrime present a strong argument for the NSTIC, which may tip the scales for privacy pragmatists in favor of the Identity Ecosystem. This does not lessen the concern that the NSTIC may actually result in decreased online security. However, people may be willing to rely on governmental assurances of security or simply support the program because the government is finally taking action. In other words, pragmatists may conclude that "something" is simply better than "nothing."

D. Minimal Intrusions Into Speech and Association

Aside from these concerns, creation of the Identity Ecosystem is likely constitutional. As related to speech, the NSTIC's policy is best placed in the realm of content-neutral regulation. The Supreme Court in *United States v. O'Brien* provided the four-part test used when analyzing

[152] Strahilevitz, *supra* note 143.

this form of legislation.[153] The Court held that, in order to remain free from unconstitutional restraint, the regulation must: 1) be within the constitutional power of the government, 2) further a substantial governmental interest, 3) be unrelated to the suppression of expression, and 4) be an incidental restriction on speech no greater than necessary to achieve the state's end.[154]

Applying these factors to the NSTIC demonstrates that the Identity Ecosystem as developed by the United States does not unconstitutionally infringe on speech. First, legislation enacting the ecosystem remains within the constitutional power of the government. The government certainly has the ability to regulate the internet. Second, the purpose of the Identity Ecosystem is abundantly clear – protection against cybercrime. Deterrence of this billion-dollar criminal enterprise certainly provides a substantial government interest, if not a compelling one. Third, the NSTIC is not designed to suppress speech or alter the freedom of expression in any way. The purpose of the NSTIC is to provide a more secure online environment, protecting public and private entities from cyber-attacks. Fourth, creation of the Identity Ecosystem results in a mere incidental restriction on speech no greater than necessary to achieve its result.

The fourth factor of the *O'Brien* test is likely the one most open to debate. Opponents to the NSTIC may argue that creation of an online identity automatically restricts speech through the chilling effect created by requiring an authenticated identity for online participation. However, this position fails for several reasons. To begin with, it is important to emphasize that, unlike *O'Brien*, which inhibited an individual from burning his Vietnam draft card, the NSTIC does not directly restrict speech in any way.[155] Next, as discussed above, the NSTIC simply provides an option for individuals to interact online. It is a safe-haven, not an all-inclusive

[153] United States v. O'Brien, 391 U.S. 367 (1968).
[154] *Id.* at 376-77.
[155] *Id.* at 369.

change, to the current on-line system. The voluntary nature and anonymity options designed within the program eliminates much of the concern, as individuals are free to create the appropriate cyber-environment that maximizes their comfort in communication. Finally, when weighed against the significant governmental interest in deterring cyber-related crime and restoring on-line security, these concerns minimal concerns are overcome. Such arguments support the conclusion that the NSTIC does not unconstitutionally infringe on a person's right to free speech or association.

E. Necessary Regulatory Measures

While the NSTIC represents a constitutional approach to a very challenging national threat, it requires certain protective legislation. The Electronic Freedom Foundation suggests that the "government would need new privacy laws or regulations to prohibit identity verifiers from selling user data or sharing it with law enforcement officials without a warrant."[156] Aside from these general concerns, there are two areas where legislation should be focused in order to protect against the constitutional concerns discussed above: 1) legislation should be enacted to protect the voluntary nature of the program, and 2) certain organizations and social forums should be given the opportunity to anonymously exist outside the Identity Ecosystem.

First, in order to protect itself from as much constitutional scrutiny as possible, the voluntary nature of the program should remain intact. Legislation should be created to reflect the "safe haven" paradigm discussed above, maintaining an environment where success of the program depends on the voluntary participation of the people at large. While the nature of the program may evolve over time, depending on the program's success, smooth transition into the Identity Ecosystem encourages adoption of a voluntary system to the greatest extent possible.

[156] Singer, *supra* note 3.

Second, as tracking certain activity within the Identity Ecosystem may result in an unconstitutional chilling of association and free speech, anonymity should also be protected. Legislation should require, at a minimum: 1) full anonymity for those who choose not to participate in the Identity Ecosystem and 2) anonymous virtual travel to sites located beyond the ecosystem's walls. Government tracking of non-participants may produce a chilling effect on otherwise protected communication and participation, particularly in the realm of political speech. Failure to allow anonymous participation in online organizations creates the same constitutional concerns posed in *NAACP v. Alabama*. Requiring an individual to adopt an authenticated online identity before virtual participation in certain forums may be viewed as synonymous with compelled production of membership lists.[157] Individuals "flagged" as nonparticipants may alter their online behavior for fear that they are being watched, thereby inhibiting otherwise constitutional speech or association. Organizations and communication forums should be given the opportunity to *anonymously* remain beyond the boundaries of the Identity Ecosystem.

Though the Identity Ecosystem represents a legitimate attempt to combat the cyber threat, the concerns posed by the NSTIC should not be taken lightly. The practical and constitutional considerations are real and potentially frightening, thereby emphasizing the need for strong oversight and regulation of this program. Failure to adequately legislate in the areas discussed above may result in an impermissible infringement on a person's rights to privacy, free speech, and association.

[157] *See generally* NAACP v. Alabama, 357 U.S. 449 (1958).

VI. Conclusion

The Federal Bureau of Investigation recently released yet another report, stating that "hackers have stolen more than 500 million financial records over the past 12 months."[158] According to the FBI, "About 35% of the thefts were from website breaches, 22% were from cyberespionage, 14% occurred at the point of sale when someone bought something at a retail store, and 9% came when someone swiped a credit or debit card."[159] As one agent warns businesses, "You're going to be hacked . . . . Have a plan."[160]

The federal government has a plan. It is called the National Strategy for Trusted Identities in Cyberspace.[161] Creation of an online Identity Ecosystem that requires a singular, robust, authenticated, online identity lies at the heart of that plan. Opponents to the NSTIC identify serious problems regarding the practicality of such a plan as well as the inherent constitutional challenges posed by a singular online identity for operations within cyberspace. These concerns are real and threatening, requiring immediate and continued attention by government officials and citizens at large. However, the doomsday approach of some opponents to the NSTIC simply overplays the reality of the Identity Ecosystem. Rather than compelling citizens to enter into an internet world that forces relinquishment of citizens' anonymity, the Identity Ecosystem merely creates an option for internet users who yearn for greater online security.

---

[158] Erin Kelly, *Officials Warn 500 Million Financial Records Hacked*, USA TODAY (Oct. 20, 2014, 8:10 PM), http://www.usatoday.com/story/news/politics/2014/10/20/secret-service-fbi-hack-cybersecurity/17615029/.
[159] *Id.*
[160] *Id.*
[161] Breeden, *supra* note 5.

It is too early to tell whether this program will survive. The NSTIC is currently in operation, but the challenges are far from resolved. Long term success will require significant oversight and federal legislation in order to protect this program from becoming exactly what privacy advocates fear most. Therefore, one should applaud those who oppose the NSTIC, as their involvement is vital to steering a proper way forward. While their efforts will likely not result in ending the program, they will ensure the Identity Ecosystem remains what it is today: a constitutional approach to a very serious problem.