JOINT COMMENTS OF

THE ELECTRONIC PRIVACY INFORMATION CENTER

and

THE LIBERTY COALITION

to

U.S. THE DEPARTMENT OF COMMERCE

NATIONAL INSITUTE FOR STANDARDS AND TECHNOLOGY

Models for a Governance Structure for the

National Strategy for Trusted Identities in Cyberspace

Docket No. 110524296-1289-02

July 22, 2011

The National Institute for Standards and Technology (NIST) within the Department of Commerce has requested public comment on governance models for administration of policy and standards adoption for the Identity Ecosystem Framework in accordance with the National Strategy for Trusted Identities in Cyberspace (NSTIC).[1] A National Program Office (NPO) has been established within NIST that is "responsible for coordinating the processes and activities of organizations that will implement the Strategy."[2]

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values.[3]

---

[1] Notice of Inquiry, *Models for a Governance Structure for the National Strategy for Trusted Identities in Cyberspace,* 76 Fed. Reg. 34,650 (Dep't of Commerce June 14, 2011), *available at* http://www.federalregister.gov/a/2011-14702 [hereinafter *Notice of Inquiry*].

[2] THE WHITE HOUSE, NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE: ENHANCING ONLINE CHOICE, EFFICIENCY, SECURITY, AND PRIVACY 37-38 (2011) [hereinafter *NSTIC*]. The NSTIC National Program Office will be tasked to "promote private-sector involvement and engagement; support interagency collaboration and coordinate interagency efforts associated with achieving programmatic goals; build consensus on policy frameworks necessary to achieve the vision; identify areas for the government to lead by example in developing and supporting the Identity Ecosystem, particularly in the Executive Branch's role as a provider and validator of key credentials; actively participate within and across relevant public- and private-sector fora; and assess progress against the goals, objectives, and milestones of the Strategy and the associated implementation activities." *Id*. at 39.

[3] EPIC, About EPIC, http://www.epic.org/epic/about.html (last visited July 11, 2011).

The Liberty Coalition is a policy interest group in Washington, D.C. The Liberty Coalition works to help organize, support, and coordinate transpartisan public policy activities related to civil liberties and basic rights.[4]

EPIC first examined legal the role of digital identities on the Internet in 1999, after Microsoft announced plans to use its Passport service to authenticate subscribers in online transactions with affiliate companies.[5] EPIC filed a complaint with the Federal Trade Commission (FTC) in July 2001. EPIC's complaint pointed out that Microsoft encouraged its users to sign up for the service and represented that the service protected privacy and complied with the Children's Online Privacy Protection Act (COPPA).[6] However, in reality Passport was facilitating the tracking and monitoring of its users by signing up all Microsoft Hotmail users for the service without the availability of an opt-out, not allowing individuals to delete their accounts, sharing user e-mail addresses with third parties by default, and neglecting key provisions of COPPA.[7]

Based on EPIC's complaint, the FTC negotiated a Consent Order that broadly required Microsoft to build in protections for the use of personal information, including e-mail addresses, persistent identifiers in cookies, and embedded identifiers, for any and all authentication systems that Microsoft offered, presently or in the future.[8] In addition, for a period of 20 years (until 2022) Microsoft is required to fully disclose all information collection and use practices, develop a comprehensive security program and obtain third-party review of it, and maintain all Passport marketing materials for FTC review.[9]

In October 2010, EPIC led a coalition of fourteen organizations, that included the Liberty Coalition, in a statement to the Department of Homeland Security in response to the Draft NSTIC document.[10] The statement pressed the Administration for a clearer definition of problems the NSTIC was meant to solve and advocated for the maintenance of a free and open Internet to protect the creative content of users, assure privacy, and ensure accountability and oversight of government activity

The organizations submitting these comments have actively followed the release and development of the NSTIC. Two of the included signatories, Amie Stepanovich and Aaron Titus, participated as speakers at the NSTIC Privacy Workshop in Cambridge, Massachusetts. Aaron Titus also co-authored a white paper reacting to the publication of

---

[4] About the Liberty Coalition, http://www.libertycoalition.net/ (last visited July 22, 2011).
[5] EPIC, National Strategy for Trusted Identities in Cyberspace (NSTIC), http://www.epic.org/privacy/nstic.html (last visited July 11, 2011).
[6] Complaint and Request for Injunction, Request for Investigation and for Other Relief: In the Matter of Microsoft Corporation, C-4069 (July 26, 2001), *available at* http://www.epic.org/privacy/consumer/MS_complaint.pdf.
[7] *See id.*
[8] Press Release, Fed. Trade Comm'n, Microsoft Settles FTC Charges Alleging False Security and Privacy Promises (Aug. 8, 2002), http://www.ftc.gov/opa/2002/08/microsoft.htm.
[9] *See id.*
[10] Elec. Privacy Info. Ctr., et al., Statement on National Strategy for Trusted Identities in Cyberspace: Creating Options for Enhanced Online Security and Privacy (Sept. 2010), *available at* http://privacy.org/privacy_coalition_comments_trusted_ids.pdf.

the NSTIC and identifiying "technology-independent privacy and security vulnerabilities that NSTIC policy must address through technology, policy, and regulation."[11] The white paper recognized that "without regulatory policy, procedural safeguards and mandatory technology standards, NSTIC will fall short of its aspirations and may do more harm than good."[12] We now welcome this opportunity to provide written comments.

I. Steering Group Structure & Function

NSTIC rightly avoids a centralized system of Internet identification managed by the federal government,[13] such as that found with REAL ID.[14] However, NSTIC must address privacy risks that accompany private sector Identity management, including protection of consumer information and implementation of strong privacy practices.

There are many instances where legislation will be necessary in order to assure a high level of protection and adequate enforcement mechanisms (see section II(a) below). In addition, a Steering Group structure with strictly defined functions is necessary in order to maintain an emphasis on privacy and consumer protection.

a. Structure: Steering Group Organization and Representation

In order to govern the Identity Ecosystem in an effective manner the NSTIC Steering Group must be regulated by procedures that protect and educate users while safeguarding privacy and promoting the guiding principles of the NSTIC.[15] The goal of the NSTIC Steering Group is to "bring together all of the interested stakeholders to ensure that the Identity Ecosystem Framework provides a minimum baseline of privacy, security, and interoperability through standards, policies, and laws."[16] NIST has recognized that the structure of the Steering Group must "support the technical, policy, legal, and operational

---

[11] AARON TITUS, TODD FEINMAN, & DAVID GOLDMAN, 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 (Identity Finder, LLC April 15, 2011), *available at* http://www.identityfinder.com/Software/Docs/IDF-NSTIC-WP.pdf

[12] *Id*. at 4.

[13] *See NSTIC*, *supra* note 2, at 4 ("The private sector will lead the development and implementation of the Identity Ecosystem, and it will own and operate the vast majority of the services within it.").

[14] EPIC, joined by 24 privacy and technology experts, submitted detailed comments in May 2007 on the REAL ID regulations. EPIC explained the many privacy and security threats raised by the REAL ID Act. In particular, the group admonished DHS for its failure to include adequate privacy and security safeguards for this massive national identification database. DHS's own Data Privacy and Integrity Advisory Committee refused to endorse the agency's plan. "The Committee feels it is important that the following comments do not constitute an endorsement of REAL ID or the regulations as workable or appropriate." The Electronic Privacy Information Center, *Comments to Department of Homeland Security on Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes* (May 8, 2007), *available at* http://epic.org/privacy/id_cards/epic_realid_comments.pdf.

[15] "The Strategy specifies four Guiding Principles to which the Identity Ecosystem must adhere: Identity solutions will be privacy-enhancing and voluntary; Identity solutions will be secure and resilient; Identity solutions will be interoperable; Identity solutions will be cost-effective and easy to use" NSTIC, *supra* note 2, at 11.

[16] *Id*. at 31.

aspects of the Identity Ecosystem without stifling innovation."[17] In order to do this, the NSTIC Steering Group must be balanced, transparent, and accountable.

The NSTIC Steering Group is proposed as a private sector entity. However, there are aspects of a legislatively created and publicly housed group that must apply to the Steering Group. The purpose, authority, and responsibilities must be set out in a charter and codified by statute, and the agency must be subject to the Federal Advisory Committee Act (FACA). The FACA establishes processes "for establishing, operating, overseeing, and terminating" advisory bodies.[18] Compliance with the FACA is vital to establishing a Steering Group that promotes transparency and public accountability. Though the NSTIC Steering Group appears to fall under the FACA requirements,[19] it is necessary to expressly establish that the rights and obligations that are imposed by FACA will be enforced against the NSTIC Steering Group. This includes that records must be maintained on costs and membership, operations must be efficient, and all records must meet transparency requirements.[20]

The NSTIC Steering Group should be modeled on the Information Security and Privacy Advisory Board (ISPAB, formerly Computer System Security and Privacy Advisory Board),[21] a FACA-compliant advisory group located within the Department of Commerce. The ISPAB was established to identify emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy, and played a critical role in defeating bad technology standards.[22] The group consists of 12 members, appointed from identified groups, and with a single member appointed as chairman.

The FACA "requires that committee memberships be 'fairly balanced in terms of the points of view represented and the functions to be performed.'"[23] In order to maximize efficiency, the core NSTIC Steering Group should consist of a correspondingly workable number of individuals. One of the individuals should be assigned a leadership role. Interests that should be represented in the NSTIC Steering Group include:

(1) Federal Government (2 representatives);
(2) Local Government (2 representatives);
(3) Private Industry (2 representatives);
(4) User and Consumer Associations (2 representatives);
(5) Privacy and Security Experts (2 representatives);
(6) Educational and Research Organizations (2 representatives).

---

[17] *Notice of Inquiry*, *supra* note 1, at 8.
[18] *Federal Advisory Committee Act (FACA) Management Overview*, U.S. Gen. Services Admin., http://www.gsa.gov/portal/content/104514 (last updated May 25, 2011).
[19] Any advisory group… that is established or utilized by a federal agency and that has at least one member who is not a federal employee, must comply with the FACA." *The Federal Advisory Committee Act (FACA) Brochure*, U.S. Gen. Services Admin., http://www.gsa.gov/portal/content/101010 (last updated Jan. 25, 2011).
[20] *Id*.
[21] 15 U.S.C. § 278g-4 (2006), *amended by* Homeland Security Act of 2002, Pub. L. No. 107-296, § 1004(1), 116 Stat. 2273 (2002).
[22] *Information Security and Privacy Advisory Board (ISPAB)*, NAT'L INST. STANDARDS TECH., http://www.nist.gov/itl/csd/sma/ispab.cfm (last updated June 20, 2011).
[23] *Id.*

Each of these groups plays a different, vital role in the development and maintenance of the NSTIC vision. Also like the ISPAB, members of the Steering Group should serve limited, staggered terms of between 2-4 years. The terms should rotate within 3 sets, with 3-5 members of the Steering Group from various groups replaced each year.

Civil Society representation within the NSTIC Steering Group is especially important. "It is important to remember that citizens direct the State rather than vice versa."[24] However, when government and business representatives gather to make decisions, the concerns of citizens are too often not represented. The governance structure of NSTIC must include representatives from civil society and should be organized in a way to promote the perspectives of civil society organizations on issues concerning online identities and authentication. As the Organisation for Economic Cooperation and Development (OECD) has found:

> "No initiatives concerned with the economic or business (or governmental) aspects of the Internet can take place in isolation from the social and cultural context of the Internet. Thus an active participation and contribution by Civil Society to discussion such as these within the OECD is not a favor granted to Civil Society but rather a necessary element in ensuring a worthwhile and productive outcome for all."[25]

In addition to having clearly defined rules, procedures must be mandated to make the NSTIC Steering Group decision-making process open and transparent. The FACA requires all meetings to be open to the public, with public notice given at least fifteen days prior to the meeting. Open meetings will secure that no Steering Group member, or group of members, is abusing their position. In addition, the NSTIC Steering Group must be required to maintain and update an online presence to provide public access to important documents and information, such as audit reports and standards guidelines, as well as documents that the Steering Group relies on in order to reach decisions.

The structure as described will assist the governance of the NSTIC for several reasons. First, the simple structure of the Steering Group will ensure that decisions can be made in a timely manner, without getting bogged down in time-consuming discussions and large-scale debates, while still ensuring that all stakeholders have a seat at the table. However, the background structure of the Advisory Board will provide a broad expanse of expertise and a support system for the Members.

b. Function: Roles and Responsibilities

A Steering Group will only succeed as an NSTIC governing body if it is empowered to protect consumer and user interests. Several sections of the NOI indicate what roles the Steering Group will perform:

---

[24] ORG. FOR ECON. CO-OPERATION AND DEV., EVALUATING PUBLIC PARTICIPATION IN POLICY MAKING 22 (2005).
[25] THE PUBLIC VOICE COALITION, FUELING CREATIVITY, ENSURING CONSUMER AND PRIVACY PROTECTION, BUILDING CONFIDENCE AND BENEFITING FROM CONVERGENCE: RECOMMENDATIONS AND CONTRIBUTIONS TO THE OECD MINISTERIAL MEETING OF 17-18 JUNE 2008, at 5 (2008).

- "…maintain the rules of participating in the Identity Ecosystem, develop and establish accountability measures to promote broad adherence to these rules, and foster the evolution of the Identity Ecosystem to match the evolution of cyberspace itself."
- "…ensure that the Identity Ecosystem Framework upholds the Guiding Principles by providing a minimum baseline of privacy, security, and interoperability through standards and policies—without creating unnecessary barriers to market entry."
- "…the steering group will administer the process for the adoption of policy and technical standards, set milestones and measure progress against them, and ensure that accreditation authorities validate participants' adherence to the requirements of the Identity Ecosystem Framework."

At the outset, the Steering Group should be tasked with specific, enumerated duties. Among these duties should be tasks specifically designed to enhance privacy protections and to protect the rights of users. Procedures must be implemented in order to prevent mission-creep and maintain focus on the core principles of the NSTIC. In this spirit, in addition to those tasks already listed, the NSTIC Steering Group should also be granted authority to meet and confer with the NSTIC Privacy Group (see section II(b) below) and to conduct studies and recommend language for legislation and regulation considered necessary for the continued success of the NSTIC program. Other duties for the NSTIC Steering Group should include maintenance of a list of approved Identity Providers; ensuring the availability of low cost identity management tools; oversight of audits for Identity Providers and Relying Parties.

II. Governance and Privacy

a. The Need for Legislation

The NSTIC makes a promise, not only to preserve, but to enhance user privacy in the Identity Ecosystem.[26] This is a commendable goal, and one that should be pursued vigorously by the National Program Office. Privacy safeguards are especially important under the NSTIC, where Identity Providers and Relying Parties will have expanded access to a wider range personal information than they even have currently, meaning that an unprotective or under-protective system is likely to have disastrous results.

Lucrative incentives to monetize personal information are a constant threat to privacy, particularly in an industry where information is highly valuable and consolidated, and alternative business models have not yet been established. As demonstrated by Clear,

[26] *See, NSTIC*, *supra* note 2, at 2 ("the enhancement of privacy and support of civil liberties is a guiding principle of the envisioned Identity Ecosystem."); *id.* at 5 ("…all of these activities occur together with enhanced privacy protections that are built into the underlying processes and technologies."); *id.* at 17 ("Individual's privacy will be enhanced."); *id.* at 37 ("…they can work to ensure the enhancement of privacy…"); *id.* at 43 ("This Strategy proposes an Identity Ecosystem that will encourage trusted online transactions, provide privacy enhancements and support civil liberties, and reduce fraud.").

the private-industry Registered Traveler program,[27] there are many dangers involved with gathering too much personal information in one place.

Clear was the largest registered traveler program in the U.S., at one point operating out of 17 airports with over 200,000 members.[28] The program allowed people to apply for a card that would allow them to pass through security faster, but required applicants to submit extensive personally identifiable information. On June 22, 2009, Verified Identity Pass, which operated the "clear" program, declared bankruptcy, and questions were raised as to what would happen with all the personal data collected.[29] Leaders of the House Homeland Security Committee sent a letter to Transportation Security Administration (TSA) asking what was going to happen with all the personal information that the program had collected on people.[30]

EPIC testified in front of the House Homeland Security Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity,[31] that the Registered Traveler database was full of errors, and that the problem was exacerbated because the database was not subject to the full safeguards embedded in the Privacy Act of 1974.[32] EPIC further testified on the danger of mission creep that occurs when a company realizes that it can derive value from using collected information for purposes other than those initially intended.[33]

The best way to protect user information in the Identity Ecosystem is through privacy legislation targeted at identity providers.[34] The NSTIC has already recognized the value of the Fair Information Practices by including them as an appendix to the document.[35] However, here is an unmistakable need to make expressly clear that these practices will be imposed as fundamental obligations on companies and organizations that

---

[27] For a later incarnation of the program, see CLEAR, http://www.clearme.com (last visited July 21, 2011).
[28] Bloomberg News, *Missing Laptop Halts Airport Program*, L.A. TIMES, Aug. 5, 2008, http://articles.latimes.com/2008/aug/05/business/fi-screening5.
[29] Alice Lipowicz, *Registered Traveler: Data Privacy, Security Prompts Chairman's Inquiry*, FED. COMPUTER WK. (June 30, 2009), http://fcw.com/Articles/2009/06/30/Concerns-over-Registered-Traveler-personal-data.aspx.
[30] Letter from Bennie G. Thompson, Chairman, House Committee on Homeland Security, to Gale Rossides, Acting Assistant Secretary, Transportation Security Administration (June 25, 2009), *available at* http://epic.org/dhs-committee_tsa-ltr.pdf.
[31] Now the House Homeland Security Subcommittee on Cybersecurity, Infrastrcuture Protection, and Security Technologies. *Subcommittee on Cybersecurity, Infrastructure, Protection, and Security Technologies*, HOUSE COMMITTEE ON HOMELAND SECURITY, http://homeland.house.gov/subcommittee-3 (last visited July 21, 2011).
[32] *Legislative Hearing on "The Future of Registered Traveler"* (Nov. 3, 2005) (Testimony of Marc Rotenberg, EPIC, to House Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, Committee on Homeland Security), *available at* http://epic.org/privacy/airtravel/rt_test_110305.pdf.
[33] *Id*. at 4-5.
[34] EPIC understands that, often, legislation needs a memorable acronym in order to gain any attention. In the interest of moving this process along, EPIC recommends the following titles to a privacy bill for Internet identities: the Privacy in the Identity Ecosystem (PIE) Act; Protecting Identity Privacy on the Internet (PIPI) Act; The Protect Online Privacy (POP) Act; Encouraging Privacy for Identities in Cyberspace (EPIC) Act.
[35] NSTIC, *supra* note 2, at app.

collect and use identity data on consumers and Internet users.[36] Effective legislation should focus on broad obligations and not security standards, opting primarily to mandate private-sector compliance with Fair Information Practices, as are already applied to the United States federal government through the Privacy Act of 1934.[37]

Fair Information Practices "provide flexible protection for privacy interests in commercial data that currently receive little or no statutory privacy protection."[38] In Europe, many countries have passed national laws based on Fair Information Practices that apply both to the public and private sector.[39] In the absence of privacy and security obligations, it is too easy for firms to continue bad practices. In fact, not only are there no incentives to change practices, but without legislation companies are likely to conceal rather than correct problems.

In addition, legislative incentives should be provided to private industry to protect personal information. In order to properly incentivize privacy-protective practices, a private right of action should be created for users who are victims of any violation of the

---

[36] In recent months, there have been many high profile data breaches in the financial sector. These breaches make clear an ongoing risk to consumers and underscore the need for stronger privacy legislation. *See*, *e.g.* Jeremy Kirk, *Citigroup Breach Exposed Data on 210,000 Customers*, PC WORLD (June 9, 2011), *available at* http://www.pcworld.com/businesscenter/article/229868/citigroup_breach_exposed_data_on_210000_customers.html; David Lazarus, *Bank of America Data Leak Destroys Trust*, L.A. TIMES (May 24, 2011), *available at* http://articles.latimes.com/2011/may/24/business/la-fi-lazarus-20110524; Taylor Buley, *Metadata: World's Biggest Data Breach*, FORBES (January 20, 2009), *available at* http://www.forbes.com/2009/01/20/data-breach-metadata-tech-security-cz_tb_0120breach.html; The Associated Press, *Wells Fargo Data Breach Revealed*, L.A. TIMes (August 13, 2008), *available at* http://articles.latimes.com/2008/aug/13/business/fi-wells13. The need to protect personal data is exemplified particularly well by the June 2011 incident where Sony Pictures websites were accessed illegally, compromising the personal information of over 1 million people in addition to the website's administrator details. The hacking group claimed all the information it obtained was left open and unencrypted, despite that Sony had already been the target of two attacks earlier in the year, against the Playstation Network and Sony Online Entertainment Networks, which "resulted in the compromise of personal data belonging to nearly 100 million account holders." Jaikumar Vijayan, *Sony Pictures Falls Victim to Major Data Breach*, COMPUTERWORLD (June 2, 2011), *available at* http://www.computerworld.com/s/article/9217273/Sony_Pictures_falls_victim_to_major_data_breach.

[37] "Fair Information Practices" (FIPs) refers to the Code of Fair Information Practices, published by the Health, Education, and Welfare Advisory Committee on Automated Data Systems in 1972. U.S. DEP'T. OF HEALTH, EDUCATION AND WELFARE, SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS viii (1973), *available at* http://epic.org/privacy/consumer/code_fair_info.html. The FIPs are embodied in the United States Privacy Act of 1974, 5 U.S.C. § 552a (2006), and are similar to the eight protections embodied in the Privacy Principles developed by the Organisation for Economic Co-operation and Development (OECD), OECD Privacy Principles, http://www.oecdprivacy.org (last visited July 11, 2011). The Fair Information Practices are referenced in Appendix A of the NSTIC as "Fair Information Practice Principles," a set of eight standards for the necessary protection of privacy in a digital environment. *NSTIC*, *supra* note 2, at Appendix A. EPIC's choice to use "Fair Information Practices" recognizes that these are protections that should be actively applied and enforced, and not aspirational principles.

[38] Letter from Privacy Coalition to Reps. Thompson and King, United States House of Representatives (Oct. 23, 2009), *available at* http://www.epic.org/security/DHS_CPO_Priv_Coal_Letter.pdf.

[39] ROBERT GELLMAN, FAIR INFORMATION PRACTICES: A BASIC HISTORY (May 13, 2010), *available at* http://www.bobgellman.com/rg-docs/rg-FIPShistory.pdf.

Fair Information Practices.[40] A private right of action would enable those directly harmed by privacy breaches to enforce Congress' intent and provide motivation for entities in the Identity Ecosystem to safeguard user privacy. A private right of action is not unprecedented – many other federal privacy laws include such provisions.[41]

b. Governance Structure

In order to assure adequate privacy protections, the NSTIC governance structure, in addition to the Steering Group and Advisory Board recommended above, should include a special sub-group that focuses exclusively on issues with privacy. The privacy sub-group would be responsible for ensuring compliance with the Fair Information Practices.

The FTC's "unfair or deceptive" regulatory structure, as it is currently situated, encourages industry to draft consumer-facing privacy policies in terms that allow for broad collection and sharing of personal information. An effective NSTIC structure must shift these incentives and persuade companies to only collect the information that is necessary for the transaction. This can be accomplished through well-structured regulation and governance.

In the place of the current system, a structure should be implemented where any entity in the Identity Ecosystem must explain to the NSTIC Privacy Group at the outset what information it seeks to collect from consumers, and why that collection is taking place. For example, an Identity Provider may collect an array of information strictly for authentication purposes, but may also want to collect consumer location and age for marketing and for research and development of new products. The application should also include details related to information disclosure, including any third parties, outside of Relying Parties,[42] with whom information will be shared. In a similar manner, Relying

[40] A private right of action must be set up to prevent Identity Providers and Relying Parties from falling into the trap of other industries, which have demonstrated a propensity to ignore regulations unless the consequences of doing so are more costly than the potential benefits of the regulated practice. *See, e.g.*, David Schmike, *Shock Treatment*, CITYPAGES (May 21, 1997), *available at* http://www.citypages.com/1997-05-21/news/shock-treatment/2 ("The FCC is the best thing that ever happened to Howard Stern. When they fine him, his ratings go up. Infinity Broadcasting dips into their little damage-control fund, pays the fine, then turns a $10 to $20 million profit in increased advertising. When he was fined $1.7 million by the FCC in 1987, Stern put out a double CD called Crucified by the FCC and made an enormous amount of money.").

[41] *See*, *e.g.*, Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681u (2006); Telemarketing and Telephone Consumer Protection Act, 47 U.S.C. § 227(b)(3), (f)(1) (2006); Drivers Privacy Protection Act, 18 U.S.C. § 2724 (2006).

[42] Relying parties should, by virtue of the FIPs, only be collecting the information necessary to authenticate the user. EPIC recommends that the Relying Party should be considered as operating within the rules and restrictions of the Identity Ecosystem until they form a binding, negotiated contractual relationship with the user as a customer (beyond the user's agreement to abide by the website's privacy policy), and at that point the terms of the contract will dictate the standards of the relationship in all future interactions after authentication has occurred. For example, a mobile phone company may require a user to authenticate his or her identity to view deals in a certain geographical area, and the information obtained as part of that authentication, or any information requested by the Relying Party after authentication has occurred, should be subject to the bounds of the NSTIC. However, once the user makes the decision to engage in business with

Parties should disclose what information they intend to request from the Identity Provider in order to authenticate a user, and why their request complies with the Fair Information Practices.

The NSTIC Privacy Group must be granted authority to approve or deny the application, or seek more information where proposed uses are ambiguous. If the NSTIC Privacy Group determines that an entity's proposal does not comply with the Fair Information Practices, including those of Data Minimization and Use Limitation, then they must be required to reject the proposal and withhold a trustmark from the entity until the entity revisits its requests. By forcing industry to disclose information policies to privacy experts up front and to justify how they comply with the Fair Information Practices, a system of accountability will be established where industry is forced to make meaningful choices regarding data collection, and will no longer be rewarded for wholesale data aggregation. In addition, this practice will not hinder innovation, since companies will still be able to collect data for clearly stated and justifiable reasons. New uses must require an additional application.[43] A breach of this application should be considered "harm" in order to prove standing in a private right of action for users (see section II(a) above).

III. Conclusion

With the proper governance structure and supporting regulations, the NSTIC is likely to be one of the most important programs in the coming decades. It is important that NIST and the NSTIC National Program Office take action now to ensure that consumer rights and consumer privacy are protected in the Identity Ecosystem and that principles of transparency and open government are complied with by the NSTIC Steering Group. The Steering Group must have a clear charter of authority, codified by statute. Also, the NSTIC Steering Group must clearly be required to comply with the Federal Advisory Committee Act, and to maintain an online presence to provide meaningful consumer access to important information about the Identity Ecosystem.

Modeling the NSTIC Steering Group after the Information Security and Privacy Advisory Board will ensure that the Steering Group can operate in an effective, efficient, and transparent manner. The Steering Group should have a limited number of members, from identified and clearly defined groups. Within the Steering Group, it is vitally important to the success of the NSTIC that civil society has a clear voice and a seat at the table.

Finally, in order to assure that the NSTIC follows through on its promise to enhance the privacy of Internet users, it is necessary to pursue legislation that will guarantee protection of lucrative personal data. In addition, a Sub-group to the NSTIC Steering

---

the carrier, and clicks on a button signifying the desire to enter personal information to the ends of entering into a contract. At this point only do the Relying Party's obligations within the Identity Ecosystem end.

[43] This may, logically, get to be a time-consuming or backlogged process, particularly when the Identity Ecosystem starts expanding. Because of this, procedures should be built in for expedited processing and pre-approval in some clearly defined cases.

Committee, focused solely on privacy, is necessary to closely monitor and audit data collection, retention, and sharing practices in the Identity Ecosystem.

Thank you,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC Executive Director

/s/ Amie Stepanovich
Amie Stepanovich
EPIC National Security Counsel

Electronic Privacy Information Center
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)

/s/Aaron Titus
Aaron Titus

Liberty Coalition
1920 L Street, N.W.
Suite 200
Washington, D.C. 20036