DOI:10.1145/1953122.1953134

Ari Schwartz

Privacy and Security
Identity Management and Privacy: A Rare Opportunity To Get It Right

The National Strategy for Trusted Identities in Cyberspace represents a shift in the way the U.S. government is approaching identity management, privacy, and the Internet.

Since 1976, when Whitfield Diffie and Martin Hellman first surmised the possibilities for the potential uses for digital signatures,[1] there has been ongoing discussion of building an online identity management structure. As use of the Internet has become more central to daily life and our financial and physical security has become intertwined with cyber security, the calls to authenticate and identify individual users have increased. However, we still have not seen a single set of answers to these issues that offer a path to an interoperable identity management system that will achieve the goals of authenticating users at different levels of risk, keeping the Internet as an innovative and growing hub for the world's interactions, and building trust among Internet users. Therefore, it is easy to be doubtful and even cynical that we can build an identity management infrastructure that is voluntary, privacy-protective, secure, and interoperable. However, over the next few years, we have a rare opportunity to build such a system, and this opportunity may be our last.

NSTIC represents only one pillar in an overall approach to resilient and effective cyber security, but it is an essential component to overall success.

Lorem ipsum dolor sit amet consect

Many countries have put forward online identity management strategies tied to centralized databases and national ID cards, but another path was clearly laid out in an important 2004 article entitled "The Accountable Net." The authors, John Palfrey, David Johnson, and Susan Crawford, suggest that the current threats on the Internet create an unsustainable situation where we risk losing the benefits of the Internet's decentralized structure. They urge us to find ways of building an Internet governance that makes peers accountable to one another as that risk is lower than the risk of empowering either an existing government or building a centralized global authority. Instead of fearing the change that will take place as the Internet becomes more accountable, those of us that love its current structure must embrace change, but also "keep the fundamental architecture and values of the Internet in mind as we do so."[2]

President Obama recognized these concerns in the release of the May 2009 Cyberspace Policy Review (CPR), which outlined the steps the public and private sector should take to overcome the risks associated with online

transactions. These actions included improving identity solutions, services and privacy-enhancing technologies, and enhancing protection for individuals' online information. [[[In response to the short-term actions laid out in the CPR, the National Strategy for Trusted Identities in Cyberspace (NSTIC) was created and was signed by the President earlier this year.]]]

As the President and his Cyber Security Coordinator have noted, NSTIC represents only one pillar in an overall approach to resilient and effective cyber security, but it is an essential component to overall success. It seeks to enhance online trust by focusing on establishing identity solutions that improve our ability to identify and authenticate the organizations, individuals, and underlying infrastructure (such as routers, servers, desktops, mobile devices, software, data) involved in online transactions. NSTIC is not only about credentials and authentication. It also seeks to limit the amount of identifying information that is collected and transmitted during the course of online transactions. This concept is clearly articulated in the NSTIC vision statement: "individuals and organizations utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation."

The Identity Ecosystem

In order to realize the vision, the strategy outlines a next generation of a trusted identity environment, the Identity Ecosystem, where individuals and organizations can operate with trust and confidence through abiding by standards and policies for identifying and authenticating their digital identities.

Four Guiding Principles establish the framework for participation in the Identity Ecosystem and form the foundation for the strategy:

▸ Identity solutions will be *voluntary and privacy-enhancing*. Individuals may choose among multiple identity providers—both private and public—and among multiple digital credentials, precluding the possibility of the creation of a national ID card or single ID database. The Identity Ecosystem will support a range of solutions that will enable limited data collection and use and distribute only relevant and necessary information about users. To accomplish this goal, it is essential to match the level of authentication to the level of risk associated with the particular transaction. The Identity Ecosystem must maintain appropriate safeguards on information and be responsive to individuals' privacy expectations tied to globally recognized Fair Information Practice Principles.[a]

a See a discussion of modern Fair Information Practice Principles in the U.S. Department of Commerce Green Paper entitled "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework" at http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf

CREDIT TK

▸ Identity solutions will be *secure and resilient*; they must stand against attack or misuse. In the Identity Ecosystem, solutions will provide reliable methods for electronic authentication that are resistant to theft, tampering, and exploitation. At the same time, credentials must be able to recover from loss or compromise and be adaptable to the dynamic nature of cyberspace itself.

▸ Identity solutions will be *interoperable*. They will be easily used by a wide variety of service providers, and they will be scalable across various boundaries, including geography, semantics, and policy.

▸ Identity solutions will be *cost-effective and easy to use*. Future identity solutions should help to reduce the complexity and the risk associated with managing multiple credentials, especially for individuals. Identity solutions should be simple to understand and enabled by technologies that are easy to use and require little training.

In order to reach these goals, not only does the government need the help of the private sector, but also the private sector must lead its implementation. In January 2011, the U.S. Department of Commerce was named the head of a National Program Office for NSTIC. As a nonregulatory agency, Commerce's job as the lead on NSTIC is to promote voluntary private sector cooperation to facilitate the growth of this Identity Ecosystem in a peer governance model similar to that recommended in "The Accountable Net."[2]

To do so, Commerce will promote private-sector involvement and engagement; build consensus on legal and policy frameworks necessary to achieve the vision, including ways to enhance privacy, free expression, and

In the age of identity theft, any project regarding identity bears close watching no matter who is running it or how it is run.

Presidential calls on IT issues, with pilot funds behind them, do not come every day.

open markets; work with industry to identify where new standards or collaborative efforts may be needed; support interagency collaboration and coordinate interagency efforts associated with achieving programmatic goals; and promote important pilots and other implementations.

There is no panacea or magic bullet to solve all cyber security issues, but leadership on an identity management can build trust, can improve security and, if done properly, can enhance privacy, but it must be led by the same type of innovators that have made the Internet what it is today. There will be an opportunity for anyone interested to participate and, it is essential that those of us that care about the future of the Internet do so if we are to be successful.

Possible Future Scenarios

I realize many will read this call to participate in NSTIC and think they have heard this concern before, but in this case, I urge everyone involved in related areas to think long and hard about the future of identity management, privacy, and the Internet. There are only a few possible future scenarios.

First, we continue on our current path. In other words, we stumble along. The market may have some good ideas on authentication that address some important Internet values: they probably will be voluntary; they may or may not protect privacy; they may be open or may be completely proprietary. In the meantime, we can expect at least a few more decades of inefficiencies, lost opportunity costs, and heavy fraud losses.

Another vision would be that governments will not wait decades and will work together or separately to begin to require identity management solutions. Although these solutions are likely to be more privacy protective, they are also likely to be more prescriptive schemes that may raise costs and make it more difficult to deliver products and services consumers want to use.

Finally, there is the NSTIC, an organized attempt to address as many issues as possible before they arise taking the leadership of the private sector and teaming it with consumer protection input from the government. It also may succeed or fail. Success has clear benefits to those who would like to ensure important aspects of today's Internet and protect privacy. Failure will put us back into one of the other scenarios.

With these options, it is clear which path is better for innovation, better for privacy, and better for openness. Certainly, in the age of identity theft, any project regarding identity bears close watching no matter who is running it or how it is run and NSTIC is no different in that respect.

Presidential calls on IT issues, with pilot funds behind them, do not come every day. There may indeed be other opportunities to develop a similar means to address related security issues while maintaining the critical values of Internet openness and privacy, but that is not a wager I am willing to make. In short, we have a chance to make a difference now. I hope you will join me and work with the U.S. Commerce Department and private sector leaders to take advantage of what may just be the last best chance to get the governance for the future of online authentication right. C

References

1. Diffie, W. and Hellman, M. New directions in cryptography. *IEEE Transactions on Information Theory IT-22*, 6 (Nov. 1976), 644–654.
2. Johnson, D.R., Crawford, S.P., and Palfrey, J.G. The accountable Net: Peer production of Internet governance. Berkman Center for Internet & Society at Harvard Law School *Virginia Journal of Law and Technology 9*, 9 (2004); http://ssrn.com/abstract=529022 or DOI:10.2139/ssrn.529022.

Ari Schwartz (ari.schwartz@nist.gov) is Senior Internet Policy Advisor at the U.S. National Institute of Standards and Technology in Gaithersburg, MD.

Copyright held by author.