WebMemo

Published by The Heritage Foundation

No. 3123
January 27, 2011

National Internet ID: Calls for Caution

Jena Baker McNeill and James Jay Carafano, Ph.D.

The White House recently took the first step toward establishing an Internet "identity ecosystem," delegating responsibility for the project to the U.S. Department of Commerce. Media reports suggest that the goal of this project is to issue unique Internet IDs to Americans that would serve as a single identifier for access to password-protected Web sites.

Before the federal government progresses too far on its project, it is worthwhile to draw some clear boundaries on what makes sense and what does not. While addressing security concerns online is important, so are protecting constitutional liberties, not hamstringing the Internet as engine of economic growth and innovation, and not unwisely expanding the power and cost of government.

An Ambiguous Plan. A draft version of the Administration's *National Strategy for Trusted Identities in Cyberspace*, published in June 2010, described an "identity ecosystem" that would consolidate the number of passwords that an individual uses to access various parts of the Web. Supposedly, by decreasing the number of passwords used, the government could decrease security vulnerabilities and help to "foster an identity ecosystem where individuals can use interoperable credentials to authenticate themselves online."

The reason for the Administration's concern is obvious: Thousands if not millions of Internet intrusions occur annually. Because of lax security on the Internet, "nation states can perpetrate espionage; industrial spies can steal trade secrets; criminals can steal money; and militaries can disrupt command and control communications."

Red Flags. Identity theft, fraud, phishing, and other malicious Internet activity should be addressed in a suitable, feasible, and acceptable manner. The federal government already has a number of ongoing cyber-credentialing activities. The Army, for example, established a public key infrastructure program to ensure more safety in military information networks. These efforts are commendable.

A government-directed national ID effort, however, raises concerns. A government-directed national ID system could:

- *Destroy online anonymity.* One of the best features of the Internet is that Americans can surf, chat, post, transact, and message anonymously. In this way, it acts as an extension of actual life where Americans freely go about their lives, largely outside the scope of government scrutiny. U.S. policies should accept the reality of anonymity, not seek to destroy it. They should focus instead on defensive solutions and deterrence that deal with and acknowledge the challenges of attribution.
- *Become the equivalent of a national ID.* Over 77 percent of the U.S. population uses the Internet. A national Internet ID system borders on creating a universal national ID—which is unneces-

This paper, in its entirety, can be found at:
http://report.heritage.org/wm3123

Produced by the Douglas and Sarah Allison
Center for Foreign Policy Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

sary and rightfully troubling to most Americans. This would raise serious concerns about the extent of government power over the Internet.

- *Crowd out private-sector efforts.* The private sector has led the way in most information technology advances over the past two decades, pioneering innovations from social networking to new security tools. An intrusive government approach to ensuring online identity could hamstring rather than promote efforts to improve online credentialing.

Next Steps. The Administration has yet to lay out how it plans to proceed. The final strategy should:

- *Focus on improving the efficiency, effectiveness, and integration of federal trusted identity programs.* The federal government must protect its own computer systems and networks. The Administration should standard for excellence, adopt best practices, and ensure that its own programs are soundly managed and integrated and are as efficient and effective as possible.
- *Develop more effective public–private partnerships to address cyber concerns.* Many federal information technologies rely on commercial off-the-shelf private-sector technology services or run on commercial networks and systems. It is imperative that government work effectively with the private sector. The public and private sectors share common challenges: Cross-talk, cooperation, sharing lessons, and establishing best practices are essential.
- *Exploit the advantages of the free market.* The government should not hamstring or limit the ability of the private sector to bring new goods and services to market that address the challenges of online credentialing.

A Risk to Liberty. It is certainly important that the federal government take the security of the cyber domain seriously. Decreasing the security risks associated with multiple credentials may well be an important and worthwhile endeavor for the private sector. However, a government-run or government-directed Internet ID system presents a risk to liberty that simply outweighs the potential security benefits.

*—**Jena Baker McNeill** is Policy Analyst for Homeland Security in the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, and **James Jay Carafano, Ph.D.**, is Deputy Director of the Davis Institute and Director of the Allison Center at The Heritage Foundation.*