Statement
National Strategy for Trusted Identities in Cybersecurity
Creating Options for Enhanced Online Security and Privacy

We thank the administration for this valuable opportunity to engage in a national conversation about privacy, and we welcome this chance to comment on the National Strategy for Trusted Identities in Cybersecurity Creating Options for Enhanced Online Security and Privacy.

The rights to free speech and free association have taken on new meaning in the Internet age. Internet users both shape and are shaped by their use of the Internet. Users are not only content consumers, but also content producers. The ability of users to generate content enriches and strengthens non-government organizations (NGOs) in two ways. First, access to the Internet is central to the ability of NGO personnel to communicate. And second, communication between NGO personnel is, in turn, central to NGO collaborative and creative opportunities.

However, the Internet also poses unique challenges for the protection of privacy and consumer rights. The open nature of the Internet creates pressing questions as to how best to facilitate Internet communications. The balance between what technologies *could* achieve and what policy *should* restrain is a delicate one. Policymakers therefore face a unique challenge – to assure that the essential freedoms of Internet communication survive while at the same time protecting user privacy and consumer rights.

The draft document states clearly that the focus is on creating an identity ecosystem that preserves the security of online transactions and supports provider choice.

Our comments regarding the draft pertain to the most pressing issues of privacy, civil liberties, and consumer rights. These issues include the need for:

- a complete enumeration of the sources of the problems identified by the draft;
- a clear plan for privacy protection;
- a strategy for the protection of private communications by fair information practices;
- the assignment of responsibility of government agencies to oversee authorities, courts, and credential users regarding constitutional rights; and
- the assurance that Internet users can continue to create, control, and own web content.

First, cybersecurity initiatives should be designed in a manner that does not discourage lawful, constitutionally protected activity. Overreaching cybersecurity measures deter individuals and organizations that rely on the Internet from engaging in constitutionally protected activities. Such activities include research,

collaboration, political participation and speech, fundraising, coalition building, campaigning, advocacy, "watchdog" activities, dissemination of information, and outreach to constituencies.[1]

Defining the Problem

At present, the draft cites security, efficiency, ease-of-use, confidence, increased privacy, greater choice, and innovation as the goals of its proposed credential requirements program. Security is indeed important, particularly for sensitive communications that involve financial information, personal health information, and human resources information, but these types of communications make up a small fraction of the volume of messages sent and received by individuals on a routine basis.

The draft's goals are valuable ones. However, the draft fails to discuss the ease with which an individual might be re-indentified or tracked when a credential system is associated with his or her personal digital device. This concern is a pressing one, because registration for a credential system necessarily requires the collection of personal identifiable information (PII).

At present, there is no great consumer demand for credential systems. Commercial attempts to develop online credential systems, such as Microsoft Passport and the Liberty Alliance, were rejected by consumers. Federal efforts to establish credential adoption and use should not create a market where one does not exist, in part because such systems place significant financial demands on Internet consumers and content providers.

We agree that there are real threats to online consumers that require additional government oversight and engagement. Identity theft, spam, and malicious code each poses serious threats to consumers. However, the draft fails to clearly articulate the connection between online ID systems and the resolution of these problems.[2] The question remains as to how a credential system will solve the problem of identity theft and malicious computer code.

Identity theft is facilitated by a number of off-line business practices regarding PII that are not addressed in the draft document. Excessive collection, retention, use, and reuse of PII by commercial actors creates identity theft vulnerabilities. Additionally, widespread institutional reliance on PII in the form of social security numbers further aggravates the incidence of identity theft.

---

[1] Cybersecurity Policy Working Group, Letter to Howard Schmidt, available at http://epic.org/privacy/cybersecurity/Cybersecurity_Letter_5-12-10.pdf, May 12, 2010

[2] White House, National Strategy for Trusted Identities in Cyberspace, June 25, 2010.

All digital privacy threats originate with the collection, retention, use, and sharing of PII. Requiring users to register for a credential can create privacy threats for users. Users wishing to engage in Internet communications without a credential should be able to do so. Content providers must not be requiring credentials at the behest of federal agencies. The grey area of what is required and what is a choice should be eliminated.

The Internet provides a vehicle for selling and sharing PII that may be used for identity theft purposes. Any credential system that is not regulated by fair information practices either through federal law, contract, or strong standards will expose users to additional privacy harms should the information shared be open for other uses.[3]

Recommendations:

1. Address the off-line systemic problems related to the abuse of PII, which would include enforcing federal law that restricts the use of the social security number for identification purposes.
2. Establish limitations on PII collection, retention, use, and reuse beyond the original purpose.

*Vulnerabilities Found in Software and Applications*

Software vulnerabilities are unavoidable contributing factors that make malicious attacks possible. Exploits like the "I Love You Virus" or "Conficker" rely upon changing the underlying code housed on a computer or digital device without the user's knowledge or consent.

Most Internet consumers are unaware that the software and firmware on computing devices may have inherent vulnerabilities that can be exploited by thieves, vandals, or the curious. These vulnerabilities can enable the collection, retention, and tracking of users. Further, such vulnerabilities can also allow damage, theft, or co-opting of digital devices for criminal or malicious activity.

These vulnerabilities also mean that unsuspecting users who make errors or use Internet-enabled technology incorrectly can cause harm to their own computer devices or those of other users.

Recommendations:

1. Provide a comprehensive description of the problems associated with the harms enumerated in the draft document.
2. Clarify the connection between certain consumer-related threats such as identity theft, viruses, or threats to privacy and the solution offered.

---

[3] EPIC, Bankruptcy of Verified Identity Pass and the Privacy of Clear Registered Traveler Data web page, available at http://epic.org/privacy/airtravel/clear/

3. Review the approaches sought to address software enabled exploits to address fundamental changes in how software is developed and certified for use in computing systems.
4. Finally, define cyber threats or crimes as intent-oriented and not outcome-driven because of the challenges posed by attribution. Fixing the underlying problems with software should be the focus for addressing many of the problems identified.

Privacy Protection

Privacy is assured by the application of fair information practices regarding the collection, retention, and use of PII. The federal Privacy Act establishes regulations regarding fair information practices that federal agencies must follow. The Privacy Act applies to federal government agency activity as it relates to the collection, retention, and use of PII.

Government policy discussions with businesses, academic institutions, or media regarding credentials may create expectations that authentication takes priority over consumer control of PII.

Recommendations:

1. There should be mandates for government-required credential systems. These mandates should include requirements that credential-issuing authorities and credential using entities (both public and private) must follow fair information practices as outlined by the Federal Privacy Act.
2. Acknowledge and address the problems for privacy that will result as a direct consequence of requiring credentials for users and content providers.
3. Ensure that the federal Privacy Act applies to credential-related information, including IP address, e-mail address, keystroke pattern recognition, user-assistive devices, browsing history, and other information that may be used to identify or re-identity an individual.

Maintenance of a Free and Open Internet

The Internet has historically been treated as a free and open media, with the ability for universal access. Government policy should be careful to continue this tradition, without creating barriers to entry in the form of fees to access certain information. Many current and past credentials programs in the private sector have charged fees for access or membership. Such fees, comparable to a "poll tax," run the risk of creating an Internet caste system, where certain government information is available only to those who can afford the credentials that are required for access.

Recommendations:

1. All standards for adequate Internet credentials should be made public in order to enable development of free and anonymous credential programs for consumers.

2. The government must be careful to avoid creating information cul-de-sacs, which would prevent universal access to information and contradict government policies of transparency and the Internet's status as a free media.

Trusted Communications Based on the Transaction

Consumers can benefit from assurances regarding transactions that involve things of value, such as online purchases. Consumers can also benefit when sensitive personal information is exchanged—such as communications with medical professionals. However, the benefit to consumers can be lost if the purpose of the trusted exchange can be compromised without Constitutional protections guarded by well-established due process mechanisms.

Recommendations:

1. Government proposals for credential systems must involve transparent and frank discussions with the Internet-using public.
2. Government should engage in full disclosure of the motivations and rationales for online identity system proposals.
3. Participation in online credential systems must be based on choice and not direct or indirect government coercion.
4. Establish transparent legal processes in advance that provide a privacy protective framework for strong due process rights for Internet users.

Accountability of Government Agencies to Independent Oversight

There is a history of government engaging in unlawful surveillance activity.

Cybersecurity activity undertaken by the federal government must be carefully monitored. Congress must accept responsibility for ensuring that all cybersecurity measures, including any mandated credential requirements program, is not abused. In order to effectively ensure the security of the system, any policies should be subject to the independent oversight of an empowered and effective Privacy and Civil Liberties Oversight Board. This body must be funded sufficiently, and it is critically important that it be staffed with a diverse group of technical, policy, and legal experts to take on the challenges of monitoring federal government activity related to cybersecurity by both civilian and military authority. Cybersecurity efforts should also be subject to rigorous public and congressional reporting.[4]

The federal courts must continue to be a source of relief for citizens. The use of national security exceptions to stop court processes should be disallowed.

---

[4] Cybersecurity Working Group, Letter to Howard Schmidt White House Coordinator, http://epic.org/privacy/cybersecurity/Cybersecurity_Letter_5-12-10.pdf, May 12, 2010

Further, the importance of whistleblowers, in both the public and private sectors, in keeping the credential system free from corruption, abuse, and misuse cannot be overstated.

Your time and attention these comments are appreciated. If you have questions or would like to engage in further discussions on the topic of credentials and online transactions, you may contact Lillie Coney, Associate Director, EPIC at 202-483-1140 x 111.

Sincerely,

Lillie Coney, Associate Director
Electronic Privacy Information Center

Shahid Buttar, Executive Director
Bill of Rights Defense Committee

Jessica McGilvray
Assistant Director
American Library Association

Sue Udry, Executive Director
Defending Dissent Foundation

John W. Whitehead, President
The Rutherford Institute

Michael Ostrolenk, Executive Director
Liberty Coalition

Tracy Rosenberg, Executive Director
Media Alliance

Alejandro Beutel, Government Liaison
Muslim Public Affairs Council

Stephen Kohn, Executive Director
National Whistleblower Center

James Landrith, Founder
The Multiracial Activist

Lisa Graves, Executive Director
Center for Media and Democracy

Dane vonBreichenruchardt, President
U.S. Bill of Rights Foundation

Tom DeWeese, President
American Policy Center

Deborah Pierce, Executive Director
PrivacyActivisim

Scholars and Experts

Chip Pitts, Lecturer in Law, Stanford Law School and Oxford University
President, Bill of Rights Defense Committee