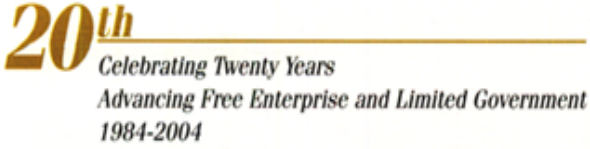
1001 Connecticut Avenue, NW
Suite 1250
Washington, DC 20036
202-331-1010
Fax 202-331-0640
www.cei.org

Federal Trade Commission
Email Authentication Summit
Comments

Written Submission of the Competitive Enterprise Institute Regarding Email Authentication

September 30, 2004



About the Competitive Enterprise Institute

The Competitive Enterprise Institute (CEI) is a nonpartisan policy analysis organization, dedicated to the principles of limited constitutional government and free enterprise. The Institute is a nonprofit educational foundation, concerned with the welfare of consumers and the economy as a whole, as opposed to one particular company or industry sector. Braden Cox is a lawyer with CEI. His specialty is e-commerce and Internet regulation. Clyde Wayne Crews, Jr. is CEI's Vice President for Policy, and has written on Internet governance issues, specifically legislative approaches toward regulating spam. He is co-editor of *Who Rules the Net? Internet Governance and Jurisdiction* (Cato Institute 2003).

Email Authentication – Market Solutions Instead of Government Mandates

Dealing with spam involves more than the annoying ritual of deleting unwanted emails. It imposes real costs in terms of time and money. Stopping spam requires both costly countermeasures by Internet service providers (ISPs) and the installation of filters that sometimes block wanted emails. Challenge-and-response systems work, but they don't stop the phenomenon of emails ricocheting throughout the Internet, and create a few problems of their own. CEI supports efforts to detect spam and holding the senders of fraudulent email accountable. However, CEI believes that heavy government involvement in the process of authentication and accreditation would harm the interests of those desiring to prevent spam. Private mechanisms are most appropriate for private networks, where problems go well beyond spam to cybersecurity itself. Private authentication mechanisms also have a role to play in protecting intellectual property—a fact that may not be taken into account, or poorly addressed, in government certification of email.

Government's role in determining authentication standards should be limited. Multiple authentication standards still vie for acceptance and dominance, and it is likely that these will coexist in the near term. Competing standards have long-term benefits despite perceived short-term costs, resulting in a more robust implementation with greater flexibility.

Government authentication would result in excessive centralization over communications. Government regulation in communications has First Amendment implications that would delay and unnecessarily politicize a technical standard. Any authentication scheme involves centralization, but government overseers have unique law enforcement powers for obtaining information that could adversely affect civil liberties in ways that private actors' information collection does not. The Commission's involvement in hosting this Summit is in itself an unprecedented foray into the technical standards setting process.

Accreditation and reputation systems involve value judgments outside the competency of government. One risk of a Summit such as this one is the possible tendency to see authentication as a way of eliminating unsolicited commercial email. But not all commercial email is bad or unwanted. In this regard, authentication will help prevent spoofing and phishing (using fraudulent emails and Web sites to fool recipients into providing personal financial data) by revealing the identity of an email's originator,

but it should not be used as a basis for *legislatively* preventing legitimate commercial email, which is a risk of governmental authentication. A system based on value judgments as to what constitutes spam would be best managed by a private body—or better yet, multiple bodies and consumers—than by a slow-moving and costly political bureaucracy.

Adoption of any authentication scheme would constitute a departure from the open nature of email transmission. While some may lament this apparent loss of anonymity, there are important distinctions. Speech is truly threatened when the government regulates it. But private efforts to limit anonymity for commercial purposes are perfectly appropriate and do not threaten free speech, properly understood. Authentication standards may "wall off" parts of cyberspace for some purposes, but the open Internet and its peer-to-peer nature remain intact.

Anonymous communication will remain possible, unless government forbids it—that is the core issue at stake in governmental deliberations over authentication. Private authentication adds to, without detracting from, the capabilities of peer-to-peer communications. Just as an authentication mandate might help the Federal Trade Commission enforce legislation such as the CAN-SPAM Act, so would requiring GPS devices in all cars help traffic police—but the costs to liberty in both scenarios are great.

For these reasons, the Commission should limit its involvement in authentication and accreditation standards to the purpose of this Summit—educating the public about email authentication.

Sincerely,

Braden Cox
Technology Counsel
Competitive Enterprise Institute
1001 Connecticut Ave. NW, Ste. 1250
Washington, DC 20036
Phone: 202.331.2254
Email: bcox@cei.org
Website: http://www.cei.org
Blog: http://www.techliberation.com/

Clyde Wayne Crews Jr.
Vice President for Policy, Director of Technology Studies
Competitive Enterprise Institute
1001 Connecticut Ave. NW, Ste. 1250
Washington, DC 20036
Phone: 202.331.2274
Email: wcrews@cei.org
Website: http://www.cei.org