



900 17th Street, N.W.
Suite 1100
Washington, DC 20006
Phone: 202.783.0070
Fax: 202.783.0534
Web: www.ccianet.org

ABSTRACT

Computer & Communications Industry Association

PRIVACY

May 2011

- *As Congress considers new regulations related to commercial data collection practices and use, provisions should be crafted in collaboration with private sector stakeholders to ensure that they do not stifle innovation or hinder legitimate business practices. Opportunities for industry self-regulation should be encouraged and safe harbors for participating companies implemented.*
- *Proposals for do-not-track requirements should be carefully scrutinized as they often represent technological mandates from the government and would serve to enshrine in law the best practices today against the privacy innovation of tomorrow.*
- *The FCC should ban network operators from using deep packet inspection (DPI) technology without explicit consumer notice and consent provisions for any purposes other than ensuring the delivery or security of data and proper functioning of the network.*

Background: Data privacy continues to present unique philosophical and practical challenges that impact business, consumers, and the government. The US approach to consumer privacy has been limited to patchwork federal statutes that include protection for specific categories of high-risk data, such as financial and medical, along with measures dealing with child online safety. This has created a framework that maintains a light touch regulation over data collection, but it can be difficult for businesses and consumers to understand. Recently, the national conversation has turned to proposals for a comprehensive federal privacy law that would cover situations outside of those specific categories.

CCIA's Position: Technological innovation and growth in electronic commerce depends upon consumer confidence. As more information is moving online, innovative services will help to bolster lower-cost, more efficient ways to connect, do business, advance learning, and provide for greater economic opportunity. Protecting the privacy of that information is crucial to retaining consumers' trust, and CCIA encourages private industry to address these concerns themselves. If companies fail to do so, the government will likely step in.

If Congress proceeds with a comprehensive federal privacy law, CCIA would look for regulations that would establish basic rules, but cautions that proposals should not discriminate or place onerous burdens on service providers that would stifle innovation. Legislative proposals should focus on going after bad actors that refuse to participate in industry self-regulation and they should reflect the delicate balance between security and freedom on the Internet.

Policy Considerations:

Information Collection and Online Targeted Advertising

Consumers enjoy a wide array of online services, such as e-mail, social networking, and

blogging platforms, and rarely have to pay for that use. Online advertising has helped to underwrite the rich variety of online content choices and services, and helps to preserve the low barriers to entry that are crucial to creating robust competition and innovation online. In this way, advertising ensures the First Amendment promises of the Internet, lowering the barrier to online speech for all consumers. Online targeted advertising also allows for sites to provide more personalized advertising by using personal information and browser activity to populate a page with more relevant ads. Safeguarding this personal information is vital for companies to retain customers, credibility and brand recognition. Internet sites know they are a click away from a customer leaving if they don't like a privacy policy.

CCIA prefers industry efforts to further develop and adhere to self-regulatory principles rather than government action. We feel that companies at the forefront of the user experience are the best equipped to provide innovative solutions to privacy problems. For example, companies are moving beyond static, multi-page privacy policies and turning to more dynamic solutions such as layered privacy notices. If Congress feels it must act, provisions should be crafted in collaboration with private sector stakeholders to ensure that they do not stifle innovation or hinder legitimate business practices. Technology continues to change rapidly and any attempt to regulate business practices will disrupt progress.

Deep Packet Inspection

Internet Access Providers (IAPs) are in a position to collect massive amounts of data on their customers' commercial and personal activity as they travel over the IAP's infrastructure, including e-mails, chats and financial information. CCIA continues to be concerned over end-user tracking conducted at the network level by Internet Access Providers (IAPs) through techniques such as Deep Packet Inspection (DPI). The lack of competition among broadband Internet access providers and the provider lock-in that comes with service contracts pose problems for consumers and businesses alike. The Federal Communications Commission (FCC) should prohibit network operators from using DPI technology and other network management techniques for any illegitimate purpose, while making clear that it is legitimate for network operators to use this technology to ensure the integrity or security of their networks.

Current Status: Online privacy has been a hot topic in Congress during the first months of 2011. Many members have either introduced legislation or announced that they are working on doing so, and Committees in both the House and the Senate are showing interest in the topic. Representatives Rush and Stearns have announced that they will reintroduce their respective bills from the previous Congress, while Rep. Speier has introduced a narrower Do Not Track bill. Senators McCain and Kerry also plan to introduce a comprehensive bill of their own. These bills generally require opt-out consent for collection of data, unless that data is sensitive or will be shared with a third party. They also allow companies to sign on to an approved industry self-regulatory effort, which gives exceptions to certain other requirements in the bill.

Both the FTC and the Commerce Department have been heavily involved in charting a new direction for the federal government on consumer privacy. Both released papers in December 2010 describing their respective visions for privacy protection and seeking comment. While not identical in implementation, the two papers both envision a comprehensive federal privacy law, based on a recognized set of FIPPs, enforced by the FTC, and that offers incentives to industries that develop enforceable self-regulatory schemes. The two differ in some pertinent details: the Commerce paper envisions an important role for the Commerce Department as a convener of industry to facilitate the development of self-regulatory programs, as well as mentioning the issues surrounding cross border data flows and harmonizing different nations' laws, for example.