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

ABSTRACT

PRIVACY

May 2010

- *Congress needs to focus on updating privacy laws to keep up with advances in technology, strengthen privacy protections for electronic communications, and set a consistent standard for government access to location data, email and private files that are stored remotely.*

- *As Congress considers new provisions related to both federal government and 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.*

- *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, integrity, or security of data and proper functioning of the network.*

Background: Data and communications privacy continues to present unique philosophical and practical challenges that impact business, consumers, and the government. The US approach to consumer privacy has historically been compartmentalized based upon industry and practice. Patchwork federal statutes include protection from potential government intrusion, electronic surveillance, and measures dealing with child online safety, creating an inconsistent framework that can be difficult for businesses and consumers to understand.

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. However, the Internet faces threats not only from hackers, but also from potentially harmful practices of the businesses and government entities that consumers rely on to protect their Constitutional right to privacy.

CCIA supports a comprehensive federal privacy law that would establish basic rules, but cautions that legislative proposals should not discriminate or place onerous burdens on service providers that would stifle innovation. Legislative proposals should focus on going after bad players and 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 online banking and some transactions require them to share information about themselves. 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. Online targeted advertising allows for sites to provide a more personalized experience by using personal information and browser activity to populate a page with 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 is supportive of industry efforts to further develop and adhere to self-regulatory principles and institute practices that put consumers first. We feel that companies at the forefront of the user experience are the best equipped to provide important services and anticipate shifts in user needs and expectations. There is broad agreement that Internet users want transparent, clear and concise details about the information being collected about them and how it is used. As a result, companies are moving beyond static, multi-page privacy policies and turning to more dynamic solutions available through popular online video sharing sites, social networking communities and other user forums to discuss privacy and security features and allow for user feedback.

As Congress considers new provisions related to both federal government and 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. Technology continues to rapidly change and any attempt to regulate business practices could 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 raise concerns 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 difficulties of changing one's provider of bundled voice/video and data services pose problems for consumers and businesses alike.

As the data becomes more commercially useful, it also becomes increasingly vulnerable to misuse by bad players and government surveillance. 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.

Government Surveillance

CCIA supports basic 4th Amendment protections against undue search and seizure, and opposes efforts to further erode civil liberties. As we have seen through the debate on the Foreign Intelligence Surveillance Act (FISA), technology is not immune to overreaching government powers. Even the best privacy policies cannot effectively prevent all undue government intrusion in the name of national security. Given the current sector-specific approach to privacy, it is unclear what standards apply to the vast new array of online applications and remote computing services (cloud computing).

Congress needs to focus on updating privacy laws, including the 1986 Electronic Communications Privacy Act (ECPA), in order to keep up with advances in technology,

strengthen privacy protections for electronic communications, and to set a consistent standard for government access to location data, email and private files that are stored remotely.

Current Status: Following last spring's hearings, Chairman Boucher (D-VA) of the House Energy & Commerce Subcommittee on Communications, Technology & the Internet and Chairman Bobby Rush (D-IL) of the House Energy & Commerce Subcommittee on Commerce, Trade and Consumer Protection have held joint hearings to explore the universal collection and use of consumer information and location information for commercial purposes. Boucher has continually pledged to work with Ranking Member Cliff Stearns (R-FL) and other House Republicans to release a comprehensive consumer privacy bill that addresses data collection and online targeted advertising and intends to include a broad disclosure requirement. Also expected to be included in the draft legislation is a tiered structure for data collection, with an opt-out provision for tracking and processing by a first party and an opt-in requirement for sharing information with an unrelated third party, if the third party is not needed for the transaction. Further, the collection and use of sensitive information that includes medical and financial information, sexual orientation identification, precise geographic location, and information concerning minors would require a consumer's express opt-in consent. The first public draft of the bill is expected this spring.

The FTC held a series of roundtable discussions to explore consumer online privacy and the challenges posed by 21st century technology and business practices. The Commission seeks to create a new framework to better protect consumer privacy while supporting beneficial uses of the information. The FTC has said that it will issue a report in June or July 2010.

In March, CCIA joined other tech companies and non-profits to form the Digital Due Process Coalition (DDP), which calls for updating ECPA. The growing use of cloud computing, cell phones and email raises issues not considered when the law was written. The DDP released recommended ECPA reform principles that call for better protection for data stored online and against bulk data requests from the government. The principles also recommend that law enforcement must obtain a search warrant before obtaining private communications or documents stored online, and before tracking peoples' location via cell phone or other devices. DDP also recommends that law enforcement submit proof that the data it seeks is relevant to a criminal investigation before electronic surveillance begins.

The Chairs of both the Senate and House Judiciary Committees said they will hold hearings on ECPA reform this spring.

In late April the Commerce Department announced a broad-based privacy-policy review and formed the Internet Policy Task Force to explore "current policy frameworks, and ways to address the challenges of the new Internet economy and society in a manner that preserves and enhances personal privacy protection." The Task Force intends to issue a report by early fall to provide policy advice to the White House.