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

January 22, 2010

FILED ELECTRONICALLY

Marlene H. Dortch, Esq.
Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: Comments - NBP Public Notice #29
GN Docket Nos. 09-47, 09-51, and 09-137

Dear Ms. Dortch:

The Computer & Communications Industry Association (CCIA) appreciates this opportunity to comment on the Federal Communications Commission's (FCC or "the Commission") Public Notice seeking comments on the relevance of online privacy protections to broadband adoption and deployment.

We believe that much of the success of the National Broadband Plan in spurring economic growth will depend on protecting consumer privacy and fostering consumer confidence. Consumer confidence is imperative for technological innovation and growth in electronic commerce.

In these comments we seek to highlight the importance of competition in driving marketplace solutions to address privacy concerns and consumer confidence. But privacy becomes a more critical issue where there is little competition and few choices, as we see with broadband Internet access providers.

About CCIA

CCIA is a nonprofit membership organization comprised of a wide range of computer, Internet, information technology, and telecommunications companies. Our members include computer and communications companies, equipment manufacturers, software developers, service providers, re-sellers, integrators, and financial service companies. Together, our members employ almost one million workers and generate nearly $250 billion in annual revenue. For over thirty years, CCIA has advocated for open markets, open systems, open networks, and full, fair, and open competition.

Competition Supports Consumer Choice

The open nature of the Internet has helped to lower the barriers to entry for small businesses and entrepreneurs to operate online, allowing consumers to benefit from and enjoy a competitive online environment that offers robust choices in online services and applications. Given this competitive online ecosystem, it is vital for companies to maintain pro-consumer practices in order 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.

There is broad agreement that Internet users want transparent, clear and concise details about what information is 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 customer feedback. For example, Facebook has used its own dynamic social network platform to announce major policy changes and has adjusted policies based on user reactions.

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. We are encouraged by reports that show Internet companies are already competing to offer their users better privacy features and security solutions. There is evidence of this in a 2009 report by the Center for Democracy & Technology that explored competition among the companies behind the five leading Web browsers in terms of their privacy settings, consumer controls, and other browser features. Also, developments over the past few years have led the three major search engine providers to revise their data retention policies to reduce the length of time that users' search records are stored. It is worth noting that tech companies have crafted data retention policies that seek to balance operational needs with privacy and security, but are often pitted between privacy advocates who favor reduced retention periods and law enforcement which favors increased retention periods and the storage of vast amounts of data.

Transparency and Disclosure

While technological innovation continues to move forward at a rapid pace, consumer expectations will also continue to evolve as more information and services migrate online. Therefore, requiring and enforcing transparency rules with full and understandable disclosure should be the first priority. This enables a healthy market to form and also empowers consumers to make informed decisions and influence companies to adopt desirable privacy policies. It also provides a mechanism to ensure that privacy standards evolve over time to meet consumer expectations.

DPI Threatens Online Privacy

Although there is a vibrant, competitive marketplace among online services, privacy becomes a more critical issue when there is little competition. CCIA continues to raise concerns with end-user tracking conducted at the network level by Internet Access Providers (IAPs) through techniques such as Deep Packet Inspection (DPI). IAPs are in a position to collect massive amounts of data on their customers' activities, both commercial and personal, as they travel over the IAP's infrastructure – from e-mails to chats to financial information. Whereas an Internet service that violates consumer trust may find consumers fleeing to a competitor, the lack of competition among broadband providers and the difficulties of changing one's provider of

bundled voice/video and broadband services pose problems for consumers and businesses alike. Many consumers cannot escape their IAP if the IAP breaches its privacy policy or otherwise violates consumers' trust. Due to the essential nature of this relationship between the consumer and IAP, and the IAP's access to all online activity, increased scrutiny and obligations are necessary.

DPI has vast implications for personal privacy and business confidentiality. If consumers feel their private information is threatened – be it by hackers, or by the businesses or network providers handling their information, or by widespread government surveillance – they will be slow to rely on broadband networks. Such reticence is directly contrary to our vision of a connected citizenry, and it is therefore essential that the Commission preserve consumer trust by limiting the use of DPI, requiring explicit consumer disclosure, and taking additional steps to build confidence in our broadband networks.

The Commission 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. It is beneficial to consumers for network operators to ease congestion as they add new capacity and to combat viruses and other network disruptions.

Data Portability and Competition

User control over their own data is critical to a well-functioning market for broadband access and Internet applications. If data is not sufficiently portable and consumers are "locked-in" to a particular service or company, they will not be able to migrate away from that product or offering in response to a change in how their personal information is handled. The Commission recognized this problem when it implemented number portability rules in the wireless marketplace. Customers should be afforded the opportunity to delete or restrict access to their data in the face of changes in a company's privacy policy.

To accommodate the flexibility needs of consumers and service providers in managing data portability issues with privacy policy changes, the Commission should recognize that there is a relationship between data portability and the reasonableness of service providers' policy changes. Where consumers can more easily port their data to the services of a competitor – that is, they can more easily "vote with their feet" – the market should more adequately discipline policy changes that are not consumer-friendly. Where consumers are locked into a service provider, however, their ability to respond to onerous policy changes is limited.

Avoid Network Filtering

We urge the Commission not to encourage IAPs to filter content that crosses over their networks. For example, over the course of many years, several congressional proposals have reflected the temptation to filter Internet content for various causes – stopping terrorism and child pornography, prohibiting "indecency," and even curbing gambling and copyright infringement. However, the Internet could die a death by a thousand cuts if IAPs must inspect transmissions, turn over customer records or block access. These proposals undermine user privacy, and threaten to erode crucial ISP immunities from liability that are critical to innovation and growth on the Internet. At a time of financial duress and economic contraction, the last thing we should be doing is attacking innovative e-commerce services that contribute to economic growth.

Protect Intermediaries from Liability

Intermediaries such as telecommunications and online service providers perform essential functions in promoting e-commerce and ensuring the continued operation of the Internet. Service providers may be a mere conduit for information, they may cache or host it, or they may provide platforms and forums for user-generated content. Because of the sheer volume of online content available today, holding telecommunications and online service providers liable for the conduct of their users would require impossible amounts of ex ante review of communications, further compromising user privacy and leading to bottlenecks in the free flow of information. Accordingly, since the 1996 Telecommunications Act, Congress has protected online intermediaries from unjustified liability for their users' actions. Due to the current trajectory of innovation in the computer and Internet industries, this takes on a heightened importance.

In addition, there is concern that platform providers or carriers may face liability for third party applications (to the extent they may ever be distinguished from content). With respect to wireless common carriers, the Commission has long-called for more openness. With freedom comes responsibility. Placing the carrier or platform operator in a position of policing applications is not the answer and could potentially impact deployment of innovative applications. Perhaps, the focus should be placed on education to inform consumers about the risks associated with an open platform environment.

Conclusion

The Commission's assessment of privacy issues should not occur independently of an assessment of market competition. Where consumers have choice and flexibility, they can select the service or application that best matches their privacy preferences. Where consumers lack choice or are locked-in, greater scrutiny may be warranted.

We encourage the Commission, in its review of online privacy issues, to avoid a one-size-fits-all approach that may prove to stifle innovation. Rather, privacy policy should encourage companies to safeguard consumer trust and discourage companies from violating that trust. Both the FCC and FTC can each play important roles in enforcing existing statutes and encouraging competition in broadband applications and online services.

Sincerely,

Edward J. Black
President & CEO
Computer & Communications Industry Association
900 17th Street, NW, Suite 1100
Washington, D.C. 20006
202-783-0070
www.ccianet.org
eblack@ccianet.org