

**TESTIMONY OF KYLE McSLARROW
PRESIDENT AND CEO
NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION**

on

Communications Networks and Consumer Privacy: Recent Developments

before the

**Committee on Energy and Commerce
Subcommittee on Communications, Technology and the Internet**

**UNITED STATES HOUSE OF REPRESENTATIVES
WASHINGTON, D.C.**

April 23, 2009

TESTIMONY OF KYLE MCCLARROW

**PRESIDENT & CEO, NATIONAL CABLE & TELECOMMUNICATIONS
ASSOCIATION**

Good morning, Chairman Boucher, Ranking Member Stearns, and Members of the Subcommittee. My name is Kyle McClarrow and I am the President and Chief Executive Officer of the National Cable & Telecommunications Association. Thank you for inviting me today to testify on “Communications Networks and Consumer Privacy: Recent Developments.”

NCTA represents cable operators serving more than 90 percent of the nation’s cable television households and more than 200 cable program networks. The cable industry is the nation’s largest provider of residential high-speed Internet service, having invested more than \$145 billion since 1996 to build two-way, interactive networks with fiber optic technology. Cable companies also provide state-of-the-art digital telephone service to more than 15 million American consumers. Cable operators are committed to delivering an open and satisfying Internet experience to their customers, and the dramatic growth in cable broadband subscribers is evidence of their success in doing so.

Our industry views the protection of our customers’ privacy as a fundamental part of our relationship with our customers and central to the success of our businesses. We operate in a highly competitive marketplace, and our ability to succeed depends on winning and retaining the trust of those customers. And as new business models and new network technologies are developed, we will ensure that they are deployed in a manner that respects our customers’ privacy.

Cable subscriber privacy is already enshrined in the Communications Act, in a comprehensive consumer protection framework that has been in effect for almost 25 years. This law –

- requires cable operators to provide annual written notice to consumers of the nature of personally identifiable information (“PII”) collected, including clearly and conspicuously describing how it is used, disclosed to others, and maintained;
- prohibits cable operators from collecting PII without prior customer consent, except as necessary to render service and detect service theft, and from disclosing PII without prior customer consent, except as necessary to render services or conduct other legitimate business activities related to rendering service;
- provides detailed requirements governing how subscriber records may be disclosed pursuant to court order;
- requires that subscribers be given access, at reasonable times and convenient locations, to all PII that is collected and maintained, and a reasonable opportunity to correct any errors in PII; and
- requires cable operators to take “such actions as are necessary” to prevent unauthorized access to PII, including destroying it if it is no longer necessary for the purposes for which it was collected and there are no pending court orders or requests for access to such information.

In addition, cable providers of digital voice service comply with the privacy protections of section 222 of the Communications Act regarding customer proprietary network information (“CPNI”).

We welcome the focus of this hearing; nearly all modern technologies – without which broadband networks could not function effectively and efficiently – have a variety of features and attributes that could implicate privacy concerns if misused. We believe the right question is what principles appropriately protect reasonable expectations of consumer privacy in a very complex online environment with many different actors. While it is certainly reasonable to examine how technologies are used, we would respectfully suggest that focusing exclusively on one particular technology – and how it *might* be misused – risks obscuring an informed and reasonable discussion of online

privacy when there are unlimited numbers of technologies and situations that could be hypothesized. What matters are the purposes for which we use those technologies and the principles by which we protect our customers' privacy. We look forward to engaging in that discussion with you.

Behavioral Advertising and Subscriber Privacy

Behavioral advertising has many advantages for consumers. Instead of a barrage of irrelevant ads, subscribers can receive information about services and offerings tailored to reflect their interests. Moreover, advertising remains a critical way to fund content and services online, often for free. Thus, advertising that is more relevant for the consumer is likely to be of more practical value to the consumer and essential to ensure the continued explosion of new content and services.

Currently, none of our cable Internet Service Providers ("ISPs") engages in behavioral advertising – that is, they do not use network-based technologies to collect behavioral data for the purpose of delivering targeted ads. But we believe that achieving and sustaining subscribers' trust requires adherence to a privacy framework that addresses four principles: first, giving customers *control*; second, providing *transparency* and *notice*; third, *safeguarding personal information*; and fourth, providing customers with *value*. And, because of the complexities involved and because the Internet is evolving so quickly, we think it is important for all industry stakeholders to work cooperatively to establish self-regulatory principles. The Federal Trade Commission's recent staff report provides a useful guide to these discussions. We look

forward to working with this Subcommittee, the FTC, and other interested policymakers and stakeholders in developing this framework.

Let me add a word here about “Canoe Ventures.” Canoe Ventures was founded last year by six of the nation’s leading cable operators to develop a national platform for delivering more relevant video advertising to cable television subscribers. These efforts are in the earliest stages, with two services slated for rollout later this year – one that does not involve the collection of any personal information through set-top boxes or otherwise, and one in which the subscriber would specifically and affirmatively consent to receiving additional information about a product or service. When and if Canoe Ventures seeks to use set-top box data to deliver behavioral ads, cable operators will do so in compliance with the privacy requirements applicable to them.

Deep Packet Inspection

As I said at the outset, what matters are the principles that should apply, not the technologies or tools that may be available today or invented tomorrow. Any technology can be used for either benign or nefarious purposes. However, given the concerns raised about deep packet inspection (“DPI”) by some of the other witnesses, I thought it would be useful to explain how cable operators actually use this technology.

Packet inspection serves a number of pro-consumer purposes. First, it can be used to detect and prevent spam and malware, and protect subscribers against invasions of their home computers. It can identify packets that contain viruses or worms that will trigger denial of service attacks; and it can proactively prevent so-called Trojan horse

infections from opening a user's PC to hackers and surreptitiously transmitting identity information to the sender of the virus.

Packet inspection can also be used to help prevent phishing attacks from malicious emails that promote fake bank sites and other sites. And it can be used to prevent hackers from using infected customers' PCs as "proxies," a technique used by criminals, in which user PCs are taken over and used as jumping-off points to access the Internet, while the traffic appears to be generated by the subscriber's PC. As a result, the technology can be used in spam filters and firewalls.

Second, packet inspection can be used for network diagnostics and capacity planning. Cable operators cannot plan for network growth without understanding how Internet traffic is growing and the uses to which it is put. By using this technology to analyze the aggregate growth and usage changes in network traffic patterns over time, cable operators can anticipate the needs of their subscribers and appropriately plan for network growth.

Third, packet inspection can help network operators accurately respond to formal requests from law enforcement agencies for the interception of communications for law enforcement purposes. When law enforcement agencies identify traffic of concern, this technology allows network operators to comply with their legal obligations to flag that traffic.

Finally, the Internet is not static. Different opportunities and challenges will emerge and this technology may prove useful in providing consumers more choice and control in ways that are difficult to predict today. For instance, as streaming video

capabilities increase, this technology could be a means of supporting more advanced parental controls.

Let me stress again that this technology – like any technology we deploy – is being deployed in a manner that respects our customers’ privacy. We believe that protection of subscriber privacy is the most useful focus for the policy debate.

Conclusion

NCTA believes that a dialogue addressing online privacy issues is healthy and a necessary component of the ongoing evolution of broadband and online services. But we respectfully suggest these discussions not be focused on one particular technology; rather, the focus should be on principles that both ensure a vibrant Internet that supports current and emerging content and services and also protect consumers’ privacy.

NCTA and its members remain committed to working cooperatively and constructively with members of this Subcommittee and other stakeholders to address these issues. Thank you again for the opportunity to appear today.