

Before the Subcommittee on Oversight and Investigations

House Committee on Energy and Commerce

Testimony of Gerard Lewis

Vice President, Deputy General Counsel & Chief Privacy Officer

Comcast Cable Communications, LLC

June 27, 2006

“Making the Internet Safe for Kids:

The Role of ISPs and Social Networking Sites”

Mr. Chairman, Ranking Member Stupak, and members of the Subcommittee:

I appreciate the opportunity to testify before you today on behalf of Comcast regarding the important subject of making the Internet safe for kids. My name is Jerry Lewis and I am a Vice President, Deputy General Counsel and Chief Privacy Officer of Comcast. My responsibilities include overseeing Comcast’s national security and law enforcement compliance and privacy efforts. I am deeply involved in Comcast’s extensive efforts to make the Internet a safe place for all our customers.

I commend the Subcommittee for its interest in and hard work on this important issue. Protecting children online is a critical responsibility in the online world and requires thoughtful and creative responses from government, non-profits and businesses alike.

1. How Comcast Protects Kids Online

Protecting the safety of children online is one of our highest priorities. Comcast is committed to providing parents with effective tools and educational materials so that they can shield their children from offensive and inappropriate content on the Internet. Since we initiated our high-speed Internet service, Comcast has worked actively with a number of leading online safety organizations to follow and refine best practices in this area.

The SafeSearch feature of our online search gives parents the ability to filter children's Internet searches to exclude sexual-themed sites. Comcast also provides all of our customers with firewall, security, and privacy and parental control software from McAfee, a leading vendor, at no additional charge. All new customers receive information about this easy to download, valuable software from the prominently featured "Security Channel" on our portal, Comcast.net.¹ McAfee is simple to use and employs enhanced content filtering techniques to give parents the power to prevent the display of unwanted and offensive Internet content. A filtering option within the privacy service enables parents to monitor chat and other activity, block inappropriate or offensive content, and prevent the sharing of personal information by their children. An event-logging feature that parents may activate chronicles lists of websites visited, websites blocked, and inappropriate chat sessions.

Comcast's "Security Channel" encourages parents to be involved in their children's online surfing experience and provides additional information not only on the McAfee service, but also hyperlinks to educational websites such as www.staysafe.org, which provide more information about child safety online. Our site also addresses various technical issues that can

¹ See <http://www.comcast.net/security/mcafee/#parental>; attached as "Appendix 1".

compromise security – for example, we caution our customers to secure their home wireless connections so that they cannot be used by others.²

While many of the companies on today’s panel function as Internet service providers (“ISPs”) and each of us plays a role as a source of evidence for law enforcement investigations, it is important to understand how our businesses differ. Unlike many of the other ISPs, Comcast does not provide extensive features or services that permit our customers to post their own content for others to see and share or to interact in real time with others. As you know, places such as online chat rooms, groups, or forums where children meet adults present some of the most serious risks. We do not provide such services for general use by our customers.

2. Comcast’s Work With Law Enforcement and Protection of Customer Privacy

Comcast works closely with law enforcement agencies to provide timely and accurate responses to their requests, and we believe that we have solid overall working relationships with those agencies. Comcast has a Legal Response team dedicated to responding to requests from law enforcement for Comcast High-Speed Internet information, and I am the lawyer who works most closely with that group. Currently, we are usually able to process and respond to law enforcement requests for information within seven business days. In true emergency situations we can usually respond to law enforcement requests in hours, and sometimes minutes. When we learn of likely incidents of child pornography or child exploitation on our network, we report these activities directly to the National Center for Missing & Exploited Children (NCMEC).

In order to cooperate effectively with law enforcement agencies, we must educate these agencies about the type of evidence they can obtain from us and how to obtain it. This past spring, we published a comprehensive Law Enforcement Guide which is distributed through

² See <http://www.comcast.net/help/faq/index.jsp?faq=Security118072>; attached as “Appendix 2”

numerous law enforcement online bulletin boards. The Guide gives law enforcement personnel the help they need to ensure that requests to Comcast are handled and processed as quickly as possible. In addition, our National Security Operations team and I meet for several hours several times each year with Department of Justice and FBI law enforcement officials based in Philadelphia and in New Jersey to exchange current information regarding cyber-crime, to obtain feedback on our law enforcement response efforts, and jointly to figure out better ways for us to work quickly and smoothly together. We are continually working to improve best practices to ensure that law enforcement receives necessary information after submitting lawful evidentiary requests. Our team is available to, and has provided, formal and informal training to law enforcement officials and I have personally provided training to law enforcement agents.

Law enforcement agents have praised our response to their requests. In the past month alone, for example, we received several letters from law enforcement officials describing the responsiveness of our Legal Response team in child abuse and child pornography investigations as “outstanding,” and its efforts as “herculean.”³ They credit our Legal Response team for having “immeasurably assisted” child pornography and exploitation investigations and for having “impacted the worlds of so many and made this world a better place.” In our most recent quarterly meeting, law enforcement officials specifically praised the speed of our processing of legal requests, and our care to produce accurate responses. While we are very proud of this feedback, neither we nor any other ISP is perfect. During a massive build-out phase of our Internet protocol (“IP”) network last year, we had significant difficulties in meeting many law enforcement requests due to problems with our customer provisioning system. That phase is behind us, and we are committed to best practices in this area.

³ The law enforcement letters appear at the end of this testimony; attached as “Appendix 3.”

We continue to seek ways to provide top-notch service in response to lawful law enforcement requests, and we also continue to expand our Internet law enforcement compliance team as our business grows.

Comcast is proud of its record assisting law enforcement when they present us with valid legal requests. But our customers should understand that we are strongly protective of their privacy and we are proud of our efforts here, too. Comcast strictly limits the kind of information it collects and retains about its Internet customers. We are extremely mindful of customer privacy, and it has been our policy and practice to collect and retain only information necessary for service delivery and network operations and management. We store this limited information for only as long as necessary for the purpose for which it was collected. We don't track or retain web page visits of our Internet customers on a personally identifiable basis, unless compelled to do so by valid legal process such as a court order, for example.

We must walk a fine line between preserving the privacy of our customers and meeting the legitimate needs of law enforcement. As a cable company, we are governed by the very strict privacy provisions of Section 631 of the Cable Act, found at 47 U.S.C. Sec. 551, and we comply with this law for our Internet service. Moreover, we were further deeply sensitized to the importance of our privacy obligations when, in early 2002, it was reported that Comcast might be caching certain web usage information on a non-personally identifiable basis— with no intention of having it identifiable to any particular customer — in order to facilitate network management. The public reaction was strong and swift, from a Member of Congress and three state attorneys general, among others. While we neither did nor intended anything wrong or in violation of the law, we acted within 48 hours of contact to cease that information collection in order to assure our customers of our privacy commitment to them. At that time, we decided to

retain IP address assignment data⁴ for the absolute minimum amount of time necessary for network management – 31 days.

We remain sensitive to striking the appropriate balance between customer privacy and law enforcement interests. We understand that our 31-day IP address retention policies places us at the low end of typical broadband industry practices. We recognize the increasing importance that this type of information plays in advancing child pornography and child exploitation investigations. Therefore, in an effort to strike the appropriate balance between accommodating valid law enforcement requests and protecting the privacy expectations of our subscribers, we have decided to implement a 180-day retention policy for this IP address assignment data. One of the reasons for this change is to provide increased support for child exploitation investigations. We are working to make sure that this new policy will take effect by September 1. We are confident that this policy will enable Comcast to become more responsive to valid law enforcement requests for IP address information.

I stress that the kind of data that we routinely retain, and that law enforcement agencies routinely request from us, is strictly limited. That data consists of IP address assignments – the “temporary number” that we assign to a personal computer connected to our network – which we are able to match up to other information provided to us by law enforcement in order to identify a suspected lawbreaker. We do not retain information on any customer’s Internet use or web-surfing habits. We will only retain such information when a law enforcement agency obtains a court order as required by law.

⁴ When a PC or other device connects with our Comcast High-Speed Internet service, it is assigned a temporary IP address. This “dynamic IP addressing” means that a customer’s PC will be assigned different IP addresses by our service over time. Dynamic IP addressing helps us to manage our network more efficiently and add new customers quickly and seamlessly.

We are committed to be a leader among ISPs in striking the right balance of interests. We were part of the first small group of ISPs to meet with the Attorney General and the director of the Federal Bureau of Investigation to initiate a dialogue on ways to make child pornography and child exploitation investigations more effective. A key topic of discussion has been the development of uniform industry policies on the length of time that ISPs should retain records of which IP address was assigned to which connected personal computer at which time. We appreciate the opportunity to be a part of this important dialogue.

3. How to Improve Child Safety Online

As the Subcommittee's hearings have made abundantly clear, both government and the private sector can and need to do more to attack the problem of online child exploitation and child pornography.

Based upon our experience, we believe that the following initiatives would contribute significantly to improving child safety online, and we hope that the Subcommittee will recommend them.

a. Improved Education of Parents and Children.

The best way to thwart child exploitation is to educate parents and children about the dangers posed by pedophiles, the importance of parental involvement in a child's Internet activities, and technology tools that help to protect children from pedophiles. Specific warnings in chatrooms, for example, can educate children who are at greatest risk. Public education is an area where the private sector has and should continue to take the lead, although government involvement is, of course, most welcome.

b. Increased Training and Technical Support for Law Enforcement Investigating Cybercrime.

In our experience, there is no more valuable investment in pursuing online predators than in adequately staffing law enforcement teams, training law enforcement regarding effective investigative techniques, and providing law enforcement with sufficient technical support to trace hard-to-find perpetrators. This is a resource question. While government must take the lead, the private sector can and should help, particularly with regard to training and forensic assistance. We are prepared to work with others in the ISP industry to provide more training to law enforcement officials, as well as direct forensic assistance to law enforcement officials tracking hard-to-find child predators.

c. Give NCMEC subpoena power

Like most others in the ISP industry, Comcast submits reports of suspected child pornography to NCMEC. However, based on testimony previously delivered before this Subcommittee, we understand that a relatively small number of reports to NCMEC lead to a prosecution. A major focus of reforms should be to make these leads yield greater results.

NCMEC functions as a national clearinghouse for reports of online child pornography and child exploitation. However, NCMEC itself does not have subpoena power and must wait for federal or state law enforcement to follow up on these leads. If NCMEC itself had subpoena authority, it would have the option of gathering evidence without the delay involved in the referral process.

d. Data preservation when entities make mandatory reports to NCMEC.

To ensure that evidence is available when law enforcement follows up on reports to NCMEC, we recommend preservation, for a defined period, of available evidence in a service provider's possession that it knows to be relevant to the referral. "Data preservation" is the retention of evidence relevant to a particular investigation for a defined period so that it can be subpoenaed by law enforcement at a later date. A data preservation requirement upon a report to NCMEC would ensure that relevant, limited data would be available to law enforcement beyond the individual data retention periods observed by individual ISPs.

e. Provision of IP address assignment data and locality information regarding the suspect in reports to NCMEC.

When service providers have relevant IP address assignment information and town and state information relating to apparent child pornography, that information should be included in reports to NCMEC. We think that this extra level of detail—which many ISPs currently provide—would facilitate referrals to the right law enforcement officials and give agents a leg up in investigations where this information is available.

We are, of course, open to considering other ways to address this deeply troubling problem, but believe that these are effective means. The entire ISP community, and application and service providers as well, must continue to devise and implement new solutions to combat child pornography and exploitation.

4. Conclusion

Protecting child safety online is a critically important responsibility that Comcast takes very seriously. We appreciate the Subcommittee's holding this series of hearings on the subject, and hope that they prompt smart, effective initiatives by both government and the private sector that will make progress in the fight to keep children safe online.