

Thomas M. Dailey  
General Counsel -- Verizon Online

Chairman Emeritus, US Internet Service  
Provider Association

Testimony before House Energy & Commerce  
Subcommittee on Oversight & Investigations

Chairman Whitfield (R-KY)

June 27, 2006

## **I. Introduction**

Chairman Whitfield, Ranking Member Stupak members of the subcommittee, thank you for the opportunity to testify here today. The people of Verizon believe that the issue of online child safety is very important and Congress can help by making some improvements in the current laws. At Verizon there is a very strong belief in our responsibility as a corporate leader to do what is right. We believe helping to protect children from online predators, and assisting law enforcement in their efforts to track down those who would exploit children through the Internet, is the right thing to do. We are a part of a quickly transforming industry moving from the old world of basic telephone service to a new world of broadband networks. Not long ago people communicated through telephone calls and the Internet was something that only a techie could understand how to use. We are now in a very different era where people connect with one another around the globe in an instant and transmit and receive images via the Internet with the click of a mouse. As remarkably beneficial and enriching as the Internet has become, there comes with this technology a darker side that includes new ways to carry out old criminal activity. Child exploitation is one example. Verizon takes the

issue of fighting child exploitation very seriously and we are here today with the goal of finding new ways to combat the spread of child pornography. We applaud the efforts of this Committee, of those at the National Center for Missing and Exploited Children, and of others in the law enforcement and ISP communities, who are dedicated to the fight against child exploitation. In this spirit, Verizon offers the following testimony.

**II. Verizon as a Network Provider and its Online Safety and Security Services**

a. Verizon's Internet Access Services Operations. Verizon is a wholesale and retail provider of communications, data and video services to a wide array of customers ranging from individual consumers to multi-national corporations. In the data world, Verizon provides two primary wireline Internet access technologies: (1) dial-up Internet access service that is provided primarily on a wholesale basis to large, consumer-focused Internet service providers; and (2) high-speed Internet access service, that is provided to retail consumer and business users. Verizon's high-speed services for consumers use digital subscriber loop ("DSL") and fiber-based (commercially known as "FiOS") technologies. Both services provide high-speed Internet access and transmission capabilities. The Verizon business units that offer Internet access services include Verizon Online, which is retail focused and currently has more than five million consumer and small/medium sized business subscribers nationally; and Verizon Business, which sells a variety of wholesale and retail Internet access services to thousands of enterprise (large) businesses and government entities.

The structure of Verizon Online's consumer Internet service differs from many in the industry. All subscribers to the company's retail consumer Internet access service,

whether DSL- or fiber-based, receive a choice of portal providers when they register for their broadband service. Subscribers can choose to receive as part of their Internet access package co-branded premium portal services from Yahoo! or MSN. The services they receive from these companies are specially designed to combine certain Verizon-provided features (such as account management tools and email) with the portal provider's own content, features and functionality (such as instant messaging, email, chat, search, entertainment and other online services). This unique blending of Internet access with portal features and services has an impact on the volume of child pornography reports Verizon refers to NCMEC, which I'll discuss further in my testimony, below.

b. Verizon Online's Safety and Security Offerings. Verizon Online makes available to its subscribers a variety of Internet security services provided by Yahoo! and MSN. Each portal provides anti-virus, firewall, anti-spyware and parental control software, which currently are provided at no extra charge to Verizon Online subscribers. In addition to making the Yahoo! and MSN security services available to its subscribers, Verizon Online offers its own, private-labeled suite of security services. This security suite includes anti-virus, firewall, anti-spyware and parental control software and is available for an additional monthly charge. Historically, Verizon Online has also made commercially available parental control software offered by CyberPatrol and Cybersitter to its subscribers at a discount off the normal retail price.

In addition to its history of providing subscribers with the tools they need to help protect themselves and their children from harmful viruses and objectionable content,

Verizon Online has also worked to help educate its subscribers about Internet threats of all kinds. The company's Safety and Security website, one of the first of its kind among network providers, gives our customers access to Internet sites designed to help parents learn about ways to protect their children online, including links to the National Center for Missing and Exploited Children's ("NCMEC") website and CyberTipline for reporting incidents of child exploitation or pornography, GetNetWise (a site dedicated to educating about dangers on the Internet), StaySafeOnline and OnGuard Online (an education site offering advice regarding the safe use of chat and community networking services). Verizon Online has participated in national events such as National CyberAwareness month, which it publicized to its subscribers, and the company periodically distributes helpful information through its newsletters on wide-ranging topics that include cyber-safety.

c. Differences Between Verizon's Internet Access Services and Other Online Services. Unlike AOL, MSN and Yahoo!, Verizon Online does not currently provide chat rooms, online forums or blog sites. Although Verizon Online has provided web hosting services targeted to business users, and storage services for all users, these services to this point have not been particularly widely adopted. Thus, because Verizon Online is primarily a network access services company, and because the vast majority of its subscribers use one of the portal services provided by its portal partners, Verizon Online sees very few complaints involving actual images of child pornography and virtually no complaints of predatory activity. It is Verizon Online's belief that complaints regarding child pornography and predation activity primarily go to the

providers of the forums in which the illicit activity takes place, e.g., chat rooms and community network sites. The few reports of actual child pornography Verizon Online has historically seen have related more to content residing on its web hosting service. The vast majority of reported child pornography incidents that Verizon Online *now* receives have been in the form of emails (largely spam-related) that the company's subscribers forward to Verizon Online's security abuse email box.

### **III. Cooperation with Law Enforcement, Case Studies and Cyber-Citizenship**

Verizon has a long history of working cooperatively with law enforcement in the investigation of criminal activity, including fighting child pornography. Through these efforts Verizon has played an important role, among other things, in securing the safe return of missing children and even in saving lives. Outside the security context, Verizon has played a prominent role in the development of cyber-citizen initiatives, online safety programs and customer education websites designed to promote the public safety at large.

a. Cooperation with Law Enforcement. Verizon as a corporation handles thousands of law enforcement subpoenas every month through its voice and data communications security organizations. In the Internet context, Verizon Online processes more than 100 criminal subpoenas a month (706 so far in 2006). The Verizon Online and Verizon Business security group work with local, state and federal law enforcement officials to investigate claims ranging from property crimes (fraud, phishing and identity theft) to threatened physical harm to child pornography. Verizon Online and Verizon Business each have dedicated personnel who work with law enforcement to respond to legal process (subpoenas, court orders and warrants) and to help law

enforcement in their efforts to identify the information they need to track down illegal activity on the Internet.

Verizon Online's security group has worked diligently and cooperatively with law enforcement across the country, and with other ISPs, on investigations ranging from post 9/11 watch-list cases to tsunami fraud schemes to tracking child predators and missing children. In one highly publicized case in 2002, Verizon Online played a critical role in tracking down and saving the life of a 13 year old Pittsburgh girl who had been abducted by a 38 year old Herndon, Virginia man named Scott Tyree. After abducting the girl, Tyree was observed in a Yahoo! chat room apparently bragging about what he had done. A participant in the chat room linked Tyree's forum discussion to stories heard on the news and reported the incident. Law enforcement tracked Tyree through Yahoo! and ultimately determined that his Internet connection showed to a Verizon IP address, meaning he likely was a Verizon Online subscriber. Working with the FBI, Verizon Online's security team was able to determine the exact location of the computer Tyree was using and provided this information to law enforcement. A waiting SWAT team then raided Tyree's Herndon condominium to find the victim tied to a bedpost but relatively unharmed. Tyree is now serving a nearly 20 year prison sentence.

The Tyree case is but one example of the successes that cooperation between Verizon security and law enforcement personnel has brought in child exploitation and endangerment cases. Verizon Online security has worked with noted Polk County Sheriff's Department investigator Charlie Gates on child predation related cases and with local law enforcement personnel across the nation. Verizon Online has also worked

closely with its ISP colleagues to locate missing children. In one case, Verizon Online and AOL teamed up to track down a runaway who was logging into her AOL instant messenger account from Internet cafés across several states. As the child logged into her AIM account, AOL and Verizon Online security personnel tracked the child's location based on the location of the Internet connection and ultimately to were able to help facilitate the child's safe return. In yet another case, the quick action of a Verizon Business security team member in processing a subpoena helped police prevent the molestation of a minor.

Finally, in a child kidnapping case, Verizon security personnel received notice from a Bridgewater, New Jersey, detective that a 5 month old child had been kidnapped from a babysitter. Verizon security performed record searches and was able to discover a series of cellular and voice over IP calls that seemed like a promising lead. Verizon's investigator then coordinated with Verizon Wireless and Sprint regarding the cellular calls and with Level 3 Communications regarding the voice over IP calls, all after hours, to set up emergency assistance for the investigating detective. The next day, the detective handling the case called to inform Verizon security that the voice over IP investigation had helped lead them to the kidnapped infant and that the child was safe. These stories are but a few examples of the things Verizon security personnel do day in and day out to help law enforcement to do its job.

b. Cyber-Citizenship Initiatives. Verizon has long been a major player in advancing cyber-citizenship principles and promoting online safety for children and all Internet users. As noted above, Verizon was one of the first major ISPs to develop an

online safety and security website that offers Verizon Online subscribers a variety of information and tools to help protect against Internet threats and parents to help safeguard their children online. Verizon was one of the founders of GetNetWise.org, a campaign and web site designed to give Internet users an easy, online resource for additional information on Internet security, include (“ICRA”) to deliver an education campaign to raise the level of awareness about content threats in our converged world. Verizon and ICRA are working cooperatively to answer parents’ questions and point them to the tools they can employ to help protect their children from harmful online content. Finally, Verizon is collaborating with i-SAFE America, Inc. on a multi-year initiative to create a powerful set of cyber-citizenship tools that educate K-12 students about responsible access to entertainment, information and online communication tools, including issues related to social networking sites, chat rooms, and online bullying.

Verizon has also participated with NCMEC and the US Internet Service Provider Association (“USISPA”) in crafting a series of industry best practices regarding the reporting of child pornography, and in finding ways to enlist the support of and to educate smaller ISPs about child pornography enforcement and reporting. The company is currently working with the Department of Justice and its task force on child pornography enforcement to look at ways in which the ISP industry can work with law enforcement to improve child pornography enforcement, whether through data preservation or retention or other means. In short, Verizon has been a prominent participant in the discussion on child pornography enforcement, and in outreach efforts involving its own customers and Internet users at large. Through these efforts, and its

ongoing work with law enforcement, Verizon has demonstrated its firm commitment to helping safeguard children on the Internet and to assisting law enforcement in pursuing those who would use the Internet to exploit children.

#### **IV. Child Pornography Reporting**

Although Verizon Online does not receive the volume of child pornography related cases as other ISPs do, the company maintains a full-time security analyst who monitors Verizon Online's abuse mail box for child pornography complaints and reports. (Virtually all reports of child pornography come to Verizon Online through its abuse email boxes). Once identified as a reportable incident under 42 USC §13032, Verizon uses the NCMEC ISP Tipline to report the incident to NCMEC. Verizon is a registered user of NCMEC's ISP CyberTipline.

While Verizon Online has always reported incidents of child pornography to law enforcement, over time its approach to assessing what is and is not a reportable incident under 42 USC §13032 has changed. Historically, Verizon Online focused its reporting on instances of child pornography images found to be housed on Verizon Online servers. Because of its role as a network provider, with no chat or forum services of its own and only a small web hosting business, the volume of reportable child pornography incidents Verizon Online has received and made has been quite small (roughly 12 over the past 6 years). We attribute this small number of cases to the fact that the circumstances under which Verizon Online subscribers most often encounter child pornography involve the use of services not provided by Verizon Online today (IM, blogging or chat/forum services), or involve websites not hosted by Verizon Online. If an Internet user

encounters child pornography when visiting a third-party site, they are most likely in our experience to report the incident to the third-party, not Verizon.

Recently, Verizon Online changed its reporting criteria to broaden the categories of child pornography complaints that it passes on to NCMEC. Verizon Online observed that the vast majority of child pornography complaints it was receiving pertained to email solicitations (often spam) relating to child pornography. In analyzing these complaints, Verizon Online concluded that the emails themselves could be viewed as facts or circumstances from which a violation of the child pornography laws was apparent under 42 USC §13032. As a result, Verizon began reporting these email complaints to NCMEC in April 2006.<sup>1</sup> Since that time, Verizon Online has filed 116 reports using the CyberTipline, the vast majority of which were in the form of emails forwarded by customers, which Verizon Online in turn forwarded on to NCMEC via the CyberTipline. The balance was child pornography related emails actually received in Verizon's own email boxes. Many of these emails contain URLs that purportedly link to content containing child pornography. None of the 116 customer complaints contained actual images of child pornography.

**V. Legislative Improvements to Child Pornography Enforcement**

Verizon supports improvements to current laws regarding child pornography enforcement, rather than the creation of new mandates. In particular, we see two areas in

---

<sup>1</sup> There was a process delay in early 2006 that interrupted Verizon Online's reporting early in the year as the company reorganized its abuse group and the reporting responsibility transitioned to a new staff member. At this time Verizon Online security also experienced network connectivity problems and delays in re-establishing its ISP Tipline account that contributed to the interruption in reporting. The connectivity issue was remedied and Verizon Online resumed reporting in April 2006.

which Congress can make significant improvements in the enforcement effort, without engaging in a wholesale re-write of existing law. First, Congress should authorize NCMEC to issue preservation requests under 18 USC §2703(f). NCMEC is not a governmental entity, yet it has been charged with the responsibility to coordinate the investigation of child pornography and related cases by law enforcement. Securing the availability of electronic data is an important element to such investigations; empowering NCMEC to request preservation immediately upon receipt of a colorable report of child pornography makes sense and would significantly expedite the process of securing potentially relevant information.

Second, Congress should clarify under 18 USC §2252A that submission by an ISP of images of child pornography as part of a bona fide report under 42 USC §13032 does not constitute the unlawful distribution of child pornography. The current statutory scheme is ambiguous on this issue and the ambiguity should be eliminated. Clarification that the submission of images as part of a report to NCMEC or law enforcement is not unlawful distribution of child pornography will encourage more ISPs to report images, and thereby facilitate investigations into the reported image. Verizon urges this Committee to clarify this point.

Finally, there has been much discussion of late on the issue of data retention in the context of child pornography investigations. The expressed position of law enforcement is that data retention may be necessary to ensure that the data necessary to enable investigators to identify the user of an IP address assigned to a particular user's Internet session is present when requested. The reason IP address assignments are useful to law

enforcement is because an IP address is often an important link between illicit conduct on the Internet and the identity of the alleged perpetrator. While the debate over data retention is still forming, Verizon's general view is that IP address assignment and customer record information collected in the normal course of business could be retained by network providers for a reasonable period of time, and if retention is required, that the period of retention should be long enough reasonably to enable law enforcement to conduct their investigations. Whether this obligation should extend to others in the Internet community is still open to debate, as is whether the period of retention should be 24 months (as has been proposed) or a shorter period more in line with the retention policies of businesses in effect today.

There are two important caveats to this position, however. First, any such data retention requirements should apply only to IP address assignment information, and it should apply only to data gathered in the normal course of business. Verizon Online believes that many network providers already capture helpful information in connection with their standard processes for providing and/or billing for services. A retention requirement for IP address assignment data currently gathered in the normal course of business may be a reasonable first step that balances the needs of law enforcement with the national desire to keep the Internet free from extensive regulation and regulation-related costs. Second, the availability of data retention should not preclude granting NCMEC the data preservation authority discussed above. Data preservation will go a long way toward protecting data that might otherwise be deleted over the passage of time between the date an incident of child pornography is reported to NCMEC and the

**TESTIMONY OF THOMAS M. DAILEY  
GENERAL COUNSEL VERIZON ONLINE  
JUNE 27, 2006**

issuance of a subpoena or other legal process by a downstream law enforcement official.

An order to preserve data will not guarantee that data will be present when requested, but it will greatly improve the chances that data which is captured will be available to law enforcement at the time it is subpoenaed.

Thank you for this opportunity to present Verizon's views on this important issue.