# COMMISSION ON CHILD ONLINE PROTECTION
# TESTIMONY OF BARBARA DOOLEY
# August 3, 2000
# San Jose, California

Good Morning,

My name is Barbara Dooley. I am the president of CIX, the Commercial Internet eXchange Association, a trade group of primarily U.S.-based Internet service providers, many with an international presence. CIX was founded in 1991 to provide the first commercial interconnection to the NSFNet that served then as the Internet's backbone. CIX continues to operate a router here in California for member companies that use it as a network exchange point for Internet traffic. CIX has many years of experience in network operations. Since its founding many Internet years ago, CIX has focused its advocacy on internetworking technologies and Internet infrastructure issues affecting Internet service providers and their customers.

My statement contains four key messages.

1. The Internet is a global, distributed network of mostly private networks that is coordinated from the bottom up. From its inception, it was designed to overcome blockages and impediments.
2. Good public policies must be technically feasible and economically reasonable. Proposed "solutions" must be weighed against their costs, which could be substantial, and their effectiveness.
3. ISPs should not be placed in a position of violating their customers' right to engage in private communications by monitoring their Internet use.
4. ISPs are ready to cooperate with law enforcement authorities and courts once criminal behavior is identified and upon receipt of appropriate and authorized notification.

Let me acknowledge from the outset that some Internet users do engage in criminal or reprehensible behavior and that some of the content available on various information sites might be offensive or even criminal. After all, the Internet both reflects and is part of human society. However, the alarm over

criminal behavior and illegal material on the Internet tends to be complicated in part because the Internet cannot be controlled by individual national governments and sovereign states.

I do not mean to paint too bleak a picture about law enforcement's challenges in this networked age. Virtually all service providers willingly cooperate with law enforcement authorities following proper judicial procedures. Providers comply with those requirements directing ISPs to turn over to police evidence of child abuse that might come to their attention. This requirement comports with many ISPs' established practices regarding child exploitation.

Furthermore, ISPs provide their subscribers access to vendors that sell content filtering software programs or provide filtering software as part of their service. In recent years, ISPs have participated in research efforts that will empower users to set standards of the types of Internet content they are willing to accept.

The Internet is a communications medium that transverses national borders. And it possesses an immediate, constantly expanding global reach. Some national governments have complaints about the Internet largely because they see national values threatened by external forces. Many of these values, policies, and practices are established by national law. Germany prohibits hate speech and the sale – anywhere - of pro-Nazi publications. France prohibits certain types of non-French language Web sites and electronic commerce transactions. The U.S. is considering legislation to prohibit Internet gambling and lotteries that are legal in other states and regions. Yet the U.S. applauds the access the Internet gives to individuals, organizations, and political dissidents around the world whose right to publish or speak is suppressed by their governments. In short, there is a broad diversity of values and laws throughout the world. The Internet will naturally reflect these social differences.

Even when there is an international consensus on a crime such as pedophilia, detection and enforcement can be very difficult because of the Internet's robust technologies, rapidly changing environment, and explosive expansion. Internet traffic is roughly doubling every three months. The total

volume of data significantly exceeds voice traffic with a widening gap between data and voice. The growth in domain names and Internet hosts is increasing proportionately. While the U.S. still dominates the Internet in terms of traffic, today more than half of the Internet's users are outside the U.S. One Internet marketing firm estimated that there are actually 550 billion documents compared to the common estimate of 1 – 1.5 billion when government, corporate, and university information is included.

Law enforcement's legitimate functions are further complicated by basic Internet technology. Within the tens of thousands of internetworked data networks, it is possible to hide illegal or offensive material under innocuous names, transfer content from country to country at a moment's notice, disguise identities, and transmit messages through perfectly innocent information sites and networks to disguise their origin. Even when an illegal site is shut down, it can easily reappear under a new name or in another country. In the torrent of global data traffic and the jungle of names, languages, and countries, it can be exceedingly difficult to locate and apprehend a lawbreaker without very specific information on his or her location, evidence of the illegal act, and access to the content. Only last week, an official of the U.S. Customs Service told the House Government Information Management Subcommittee that more than 100 countries do not have the necessary laws to deal with computer-related crime. In the borderless world of cyberspace, if countries do not coordinate their efforts, the result might be that criminals go unpunished.

ISPs are not in a position to substitute for law enforcement authorities. Unlike telephony, in which a telephone call over a wire goes from one point – home or business – to another home or business, the Internet is a connectionless medium. On the Internet, packets of data are routed across multiple routes and networks to be reassembled at the terminating end. Individual packets do not make sense until they are reassembled. In the future, as encryption becomes widely used, it will become more and more difficult to comprehend intercepted Internet traffic.

Beyond these technical challenges lie a host of other issues. ISPs cannot physically monitor the flood of data coursing through their networks. Even if they could, ISPs should not be placed in the position of monitoring their customers, violating their rightful expectations of privacy or making questionable legal or value judgments about customers' Internet usage.

It has been my experience that ISPs have been open to working with law enforcement authorities as long as the initiatives requested are legal. In closing, I should stress that it is imperative that any proposed solutions to criminal activity over the Internet be technically feasible and economically reasonable. Technically infeasible proposals that are inconsistent with the Internet's architecture or are designed primarily for public relations purposes are doomed to failure. Policies that impose high, disproportionate costs on ISPs will burden them and, in the process, slow deployment of the Internet.

I look forward to active and continuing discussions among all stakeholders so that we can increase understanding of all our concerns and arrive at mutually satisfactory solutions. I am prepared to answer any questions you have.