Statement of Paul Misener,
Vice President for Global Public Policy, Amazon.com, Inc.

Testimony Before the

Subcommittee on Communications
Senate Committee on Commerce, Science, and Transportation

Hearing on Internet Security / Hacker Attacks

March 9, 2000

My name is Paul Misener, and I am Amazon.com's Vice President for Global Public Policy. Amazon.com opened its virtual doors in July 1995 with a mission to use the Internet to transform book buying into the fastest, easiest, and most enjoyable shopping experience possible. Today, Amazon.com also offers consumer electronics, toys, CDs, videos, DVDs, home improvement tools, and much more. Seventeen million people in more than 160 countries have made us the leading online shopping site.

Amazon.com greatly appreciates the opportunity to testify before your subcommittee on the recent distributed denial of service attacks. We look forward to working with Congress to address these incidents and other important Internet policy issues. Because electronic commerce is the driving factor in the current booming economy, our nation's economic well-being depends in part on stopping illegal activity that impedes e-commerce.

We particularly support the federal government's involvement in fighting criminal behavior on the Internet. We recognize and appreciate, however, your subcommittee's important role in overseeing communications commerce.

Mr. Chairman, although the distributed denial of service incidents that occurred last month have been described many times in the press and elsewhere, a short description of what specifically happened to Amazon.com bears repeating.

In essence, for about an hour on February 8, 2000, a large amount of so-called "junk traffic" was directed to our Internet site. This junk traffic degraded the technical quality of service at the site.

To be clear: this was not a break-in at our online premises but, rather, a deliberate and illegitimate crowding of the virtual "driveways and sidewalks" around our online store. This crowding somewhat hindered our customers' ability to visit and shop.

At all times during this crowding, however, our customers' information was safe and secure, and many customers were able to enter and shop at our store. Nonetheless, for about an hour, our customers experienced congestion-related delays when visiting the site. For Amazon.com's customers, who have come to expect the world's best online shopping experience, even such a relatively minor inconvenience was frustrating.

This is a key point for these hearings: *consumers* are the ones inconvenienced by distributed denial of service attacks. Indeed, millions of consumers have come to rely on the Internet to communicate, shop, invest, obtain news, and learn online. The denial of service attacks last month interrupted these important consumer activities and, thus, it is on behalf of consumers that all of us must work to prevent these attacks in the future.

So what can the federal government do about denial of service attacks? Amazon.com believes the government's key role should be to prosecute the perpetrators of these and other

online criminal activities. Current laws have been used successfully in recent cases. In addition, some have suggested extending existing law or enacting new laws, and others have suggested establishing stiffer penalties under existing statutes.

On behalf of our current and future customers, Amazon.com would be happy to work with Congress on any new legislation to address Internet crime issues.

Successful prosecutions, of course, also rely on adequate resources with which to conduct investigations. Amazon.com believes that additional resources should be applied in at least four areas: law enforcement training, personnel retention, public education, and agency coordination. Let me say a few things about each area.

First, continuous training of law enforcement personnel in the latest digital forensic techniques, as well as current Internet technologies, should be at the top of any list for additional funding. In particular, additional training in electronic evidence handling is necessary, for preservation of digital evidence is as important for cyber crime prosecutions as preservation of fingerprints is for physical crimes.

Second, given the strong demand for information technology experts, both within and outside of government, law enforcement agencies need additional resources to retain senior IT professionals and attract new ones.

Third, federal law enforcement agencies should have sufficient resources to help educate private industry and consumers on preventing Internet-related crime.

Finally, better coordination and communication among federal, state, local, and international law enforcement agencies is needed. The recent incidents were not geographically

localized, and there is no reason to expect future Internet crime to be.

In all of these areas, increased government interaction with private industry would help. Amazon.com already is engaged in this sort of informal partnership: in addition to assisting the ongoing investigations, our technologists are working with various law enforcement personnel on the latest developments in Internet technology and techniques. We believe it would be premature, however, to formalize this partnership.

Absent from our suggested federal response is a role for the Federal Communications Commission. The reason is straightforward: the distributed denial of service attacks involve coordinated and criminal transmission of content over the Internet. It is hard to see how the FCC has statutory authority over such matters. Yet even if it had, or were given, such authority, the agency currently lacks the resources and expertise to do what is necessary at this point, namely, to fight the criminal activity. Simply put, useful FCC involvement would require statutory changes, additional resources, and additional expertise to succeed. This is work better left to law enforcement agencies.

In conclusion, Mr. Chairman, we applaud your effort to address these denial of service attacks and to formulate an appropriate federal response. As indicated, we believe the situation currently is best handled using law enforcement mechanisms, but we would appreciate your subcommittee's continued interest in the matter. On behalf of our current and future customers, Amazon.com stands ready to help.

Thank you very much for the opportunity to testify before your subcommittees. I would be pleased to answer your questions and I look forward to working with you.

* * * * * *