

Hearing of the Senate Subcommittee on Science, Technology and Space
“Holes in the Net: Security Risks and the E-Consumer”
Sen. Ron Wyden – July 16, 2001

- I last chaired a Congressional subcommittee in the early 1990's when the Internet was not part of anyone's jurisdiction. Given how dominant the Internet is today in our lives, I think it's appropriate to look back for just a minute.

- Not very long ago, the Senate Committee on Commerce, Science and Transportation had a very different purview. Commerce in the United States largely involved the physical movement of goods. This Committee was charged with writing the ground rules for an economy where millions of workers – most of them men – got up at the crack of dawn, ate thousands of calories for breakfast, and moved those goods from one point to another.

- Today, commerce has changed, and there is an increasing role for the movement of ideas and goods through packets of light. I feel strongly that it makes no sense to try to shoehorn the new challenges of a technology-driven economy into rules and policies written for another time. Therefore, a special priority of this subcommittee will be to examine fresh, creative ideas for a world driven by information technology.

- The purpose of today's hearing is to examine how the Internet has changed since its inception, and to look at the security risks and vulnerabilities that have developed along with the rise of e-commerce.

- Everyone reads in the newspaper about occasional virus attacks, computer glitches, and hacker mischief. But today this subcommittee is fortunate to have witnesses who can look beyond individual incidents and help provide perspective. Specifically, what risks are introduced as Americans move more and more critical business functions onto the Internet? And what can be done to minimize the risks?

- **The Internet is not risk-free, but this Subcommittee will show there are practical steps the public can take to make the open house of the Internet a safer house – and not a house of cards.**
- Things have certainly changed since the inception of the Internet. The World Wide Web has evolved from a platform for researchers sharing information, to an entertaining and useful vehicle for “surfing the Web,” to a core medium for American commerce.
- “Hacking” is no longer a joke, a mischievous prank that teenagers pull for fun. Where e-commerce is concerned, “sabotage” would be a better term. As we explore this issue today, there are several elements I want to emphasize.
- First, the Senate should keep its eye on the principal challenge: overcoming obstacles to electronic commerce. That’s what I’ve tried to do with the Internet Tax Freedom Act, the Digital Signatures law, and the Y2K liability legislation. I see reducing risk for the e-consumer as continuing the effort to overcome obstacles to e-commerce.
- The job’s not going to get done by taking an ostrich approach to security issues and pretending there aren’t risks. I believe when consumers and businesses understand fully what those risks are and how to minimize them, they will shift more business functions to the Internet – and that’s what I hope this Subcommittee can promote.
- It’s important to do this now because our lives are increasingly intertwined with the Net. Our mobile phones connect us. Our personal digital assistants connect us. Our home appliances may be soon be connected to order new groceries or detergent.
- With this growth, there will be an increase in the array of attacks against the Net. Even now, there is already emerging a sort of “hacker hierarchy” allowing two very different kinds of people to damage e-commerce. Most problems originate with a small minority of people who are not

technology simpletons. But their work is now available Internet-wide. Programs today are sophisticated enough to provide a hacking how-to for folks who couldn't manage it alone.

- There are a number of ways government can buttress e-commerce security efforts in the private sector. Law enforcement can provide the tools to track down attackers and the consequences that will discourage them.
- Since people, not programs, will be ultimately responsible for making the Internet more secure, government can encourage education and incentivize research and development of security services. Government can also facilitate information-sharing that might not otherwise occur in the private sector, fostering discussions to identify the best practices that might better serve the public Internet-wide.
- The New York Times reported recently that companies providing Internet security are still booming, despite an overall slowdown in the high-tech sector. I hope our witnesses today will be able to tell us what risks exist, what precautions can realistically achieve, and how businesses and consumers can best meet the security challenges of e-commerce.
- Today, we have an excellent panel. Dr. Vinton Cerf is Senior Vice President for Internet Architecture & Technology at WorldCom and is known as one of the fathers of the Internet. Mr. Harris Miller is President of Information Technology Association of America, a trade association representing the broad information technology industry. Finally, Mr. Bruce Schneier is Chief Technology Officer of Counterpane Internet Security and the author of Secrets and Lies: Digital Security in a Networked World. I've asked that you limit your statements so we'll have plenty of time for questions. Your full written testimony will be made part of the record. First, Dr. Cerf.