ORAL STATEMENT OF
COMMISSIONER JON LEIBOWITZ
before the
Committee on Commerce, Science, and Transportation
U.S. Senate
on
Data Breaches and Identity Theft
June 16, 2005

Good morning, Mr. Chairman and Members of the Committee.

We were all stunned to learn about the Citigroup computer tapes with customers' personal data that recently were lost during UPS transit. But what struck me most was a remark by one privacy advocate in a *New York Times* story. She said:

> "Your everyday dumpster diver may not know what to do with these tapes, but if these tapes ever find their way into the hands of an international crime ring, I think they'll figure it out."

Let's hope by now these tapes are either buried deeply in a landfill – or they are soon recovered untouched. But the truth is that consumers' personal information is being compromised every day – and that the data security problem is not confined to U.S. borders.

Indeed, American consumers routinely divulge personal information to foreign websites. They routinely share credit card numbers with telemarketers from around the world. And they routinely receive spam from distant corners of the globe.

Let me share just a few disturbing scenarios with you:

- A foreign website selling to U.S. consumers states that "we take all reasonable steps to safeguard your personal information." In fact, the company takes no such steps and posts sensitive consumer data in a publicly accessible manner.

- Thieves from Eastern Europe use spyware to track U.S. consumers' keystrokes as they shop over the Internet.

- Overseas telemarketers obtain U.S. consumers' bank account information under false pretenses (that's called "pre-texting") and use it to wipe out their accounts.

Sadly, these examples are based on real FTC investigations[1] – many of which, unfortunately, are difficult to pursue because of limits on our ability to exchange information with foreign law enforcement partners.

Mr. Chairman, the Commission expects to issue a Report later this summer that details the harm caused by trans-national fraud and the serious challenges we face in investigating these international cases. Foreign law enforcement agencies may be unwilling to share information with the FTC because we cannot sufficiently guarantee the confidentiality of that information. And we are prohibited from sharing certain information we obtain in investigations with our foreign counterparts – even if they want to help us and even if sharing information would help stop fraud against U.S. consumers.

To be sure, there is no panacea for the problems of international data security breaches. But legislation allowing us to exchange information with foreign law enforcers under appropriate circumstances would be a significant step forward.

The bottom line is this: if you want the FTC to be more effective in stopping spam, spyware, and security breaches, you need to give us the tools to pursue data crooks across borders.

Mr. Chairman, I won't go into detail about the legislation. I know that you are looking at a draft of the bill, for which we are grateful. The draft is almost identical to the non-controversial measure Senators McCain and Hollings moved unanimously through your Committee and the Senate in the previous Congress. It still includes those minor changes made last year to address the concerns of industry and privacy groups.

Again, thank you for your willingness to listen to us today. Along with my colleagues, I'd be happy to take any questions.

---

[1] We have changed some facts to protect the confidentiality of our investigations.