Remarks for Lydia B. Parnes
Safe Harbor Workshop
December 7, 2005

Thank you. I am Lydia Parnes, Director of the Bureau of Consumer Protection at the Federal Trade Commission, just a few blocks down Pennsylvania Avenue from where we are sitting today.

I would like to start by thanking the Department of Commerce and the Article 29 Working Party for organizing this event. When I traveled to Brussels last June to meet with the Working Party, I was given a very warm welcome and I am pleased that we have the opportunity here in the United States to reciprocate.

It is also wonderful to see so many members of industry. It looks like we have reached "standing room only" here today. This impressive turnout demonstrates the importance of the Safe Harbor framework and the commitment of companies in the United States to be responsive to the needs of our friends across the Atlantic.

Thank you Mr. de la Loyere for your presentation on the European approach to data protection. As all of you in this room know, Europe and the United States have different approaches. But we do share a

common goal: protecting the privacy of consumers. Workshops like this one demonstrate that we have found ways to bridge our differences, and I am confident that we will continue to do so. Bridging differences in our approaches is important because increasingly, cases involving consumer privacy contain a cross-border element. Thus, not only do we need to continue our dialogue, but we will need to cooperate with one another in enforcement efforts. In fact, I know that the United States government and the governments of many European countries are participating in the OECD's work plan on privacy enforcement cooperation through one of its working parties. We are excited by this work and believe that we can see positive results from this collaboration.

In the United States, our approach to privacy is one that combines legislation to protect certain types of sensitive information, aggressive enforcement, self-regulation, and consumer and business education. Each of these four elements plays an important role, and together, they create a framework that strives to achieve what we believe is at the core of consumer privacy: Preventing Consumer Harm.

I. Legislation

First, let me briefly touch upon the legislative framework for privacy in the United States. We do have privacy laws that protect information about consumers held by government agencies. Generally, these laws prohibit the unauthorized disclosure of information about individuals, and give consumers the right to:

- review records about themselves
- find out if records have been disclosed, and
- request corrections or amendments of these records.

In fact, the Federal Trade Commission is required to comply with these laws.

We do also have a federal law that serves as our backbone in protecting consumer privacy in the commercial arena – – the Federal Trade Commission Act. The FTC Act, our general consumer protection statute that prohibits unfair or deceptive acts or practices, gives us the authority that we need to file cases against companies that are engaged in unfair or deceptive acts or practices in the area of consumer privacy.

To supplement the FTC Act, we have privacy laws designed to protect the most sensitive consumer information. Let me give you a few examples:

The information about consumers held by financial institutions – like banks, mortgage brokers, and credit card issuers – includes not only name and address, but also social security number, household income, and asset information. We have legislation that places certain restrictions on the ability of financial institutions to share this information and that requires financial institutions to adequately safeguard this information. This legislation was passed in response to a recognition that consumers could be significantly harmed by the misuse of this sensitive information.

Another example is information about children. We do have legislation that requires companies to obtain parental consent for the collection or use of any personal information about children. This legislation, which went into effect in the year 2000, was passed in response to a growing awareness of Internet marketing techniques that

targeted children and a recognition that significant harm could result if information about children was misused.

There are a number of other pieces of legislation that protect consumer information in specific areas, including medical information and credit information. Again, these laws are designed to prevent the harm that can result when this type of information is misused.

II. Enforcement

A legislative framework, however, can only add value if there is adequate enforcement – and enforcement is at the heart of our approach to privacy. Through these enforcement efforts we strive to protect consumers and deter companies from engaging in activities that cause consumer harm. Under the FTC Act, our cases involve false security claims, the failure to maintain adequate security safeguards, and the failure to abide by privacy representations. We have also brought cases challenging violations of the sector-specific laws that protect sensitive information.

A. Enforcement under the FTC Act

1. False security claims

In the information security area, we have filed numerous cases challenging false security claims under Section 5 of the FTC Act alleging that companies promised that they would take reasonable steps to protect consumers' sensitive information, but failed to do so. In these cases, we allege that these false security claims constitute a deceptive act or practice. For example, last year we filed a case against Petco – a national seller of pet food and other pet related products and services. Petco's website had a number of security flaws and – contrary to the claims they made on their website – they did not take reasonable or appropriate measures to prevent unauthorized access to consumer records, including credit card numbers. The misuse of this kind of information can cause real consumer harm. The settlement in this case requires Petco to implement a comprehensive information security program for its Web site.

2. Unfairness

Petco involved a failure to abide by representations that consumer

information would be secure. But, we have also brought actions when companies did not make any representations about the safeguarding of consumer information. In these cases, we used our unfairness authority to challenge companies that fail to employ reasonable and appropriate security measures to protect the information they store.

For example, in the DSW case – – a case we announced just last week – – the FTC alleged that this shoe discounter's failure to take reasonable security measures to protect sensitive customer data was an unfair practice that violated the FTC Act. DSW's failure allowed hackers to gain access to the sensitive credit card, debit card, and checking account information of its customers. This resulted in real consumer harm. The FTC charged that a total of approximately 1.4 million credit and debit cards and 96,000 checking accounts were compromised, and that there have been fraudulent charges on some of these accounts. The settlement requires DSW to establish and maintain a comprehensive information security program that includes administrative, technical, and physical safeguards. The settlement also

requires DSW to obtain, every two years for the next 20 years, an audit from a qualified, independent, third-party professional to assure that its security program meets the standards of the order. Violations of this order may trigger civil penalties.

These FTC actions do more than affect the security practices of one company. They make the statement "we are watching you." And while companies like publicity, they do not welcome the negative publicity that accompanies a security breach and a call or letter from the FTC. And so, our hope in continuing to bring these security cases is that the safeguarding of consumer information will be improved at all companies – – not just the ones who have been on the other side of an FTC enforcement action.

3. Other Privacy cases

Our privacy enforcement, however, has not been limited to cases involving security practices. We have also used our authority under the FTC Act to bring cases that involve the misuse of personal information. In one case, the FTC alleged that Gateway Learning Corporation rented

out personal information about consumers to other companies. This practice was contrary to the promises it made in its privacy policy. The FTC also alleged that, after collecting consumers' information, Gateway Learning changed its privacy policy to allow it to share the information with third parties without notifying consumers or getting their consent. This was the first FTC case to challenge deceptive and unfair practices in connection with a company's material change to its privacy policy. Under the settlement we reached, Gateway Learning is barred from making deceptive claims about how it will use consumers' information and from applying material changes in its privacy policy retroactively, without consumers' consent. It also requires that the company give up the money that it earned from renting the consumer data.

In another case, an Internet company that provided shopping cart software to online merchants rented personal information about merchants' customers to marketers, knowing that such disclosure contradicted merchant privacy policies. In this settlement, the company is barred from using the personal data it had already collected, and from

making any future misrepresentations about the collection, use, or disclosure of personally identifiable information. The settlement also requires the company to ensure that consumers receive a clear and conspicuous notice before their personal information is disclosed to other companies for marketing purposes. Finally, the settlement requires that the company give up the fees it made by renting the consumer information.

B. Enforcement of other legislation

All of the cases I have just discussed have been brought using our general authority under the FTC Act. The FTC also enforces laws that protect certain types of sensitive, personal information. For example, the Gramm-Leach-Bliley Act is the law that protects information about consumers held by financial institutions. In our GLB cases, we alleged that mortgage companies failed to safeguard consumer information as required by the Gramm-Leach-Bliley Act's Safeguards Rule. In two of the cases, we also alleged that the companies failed to provide its customers with the required privacy notices – – the notices that provide

customers with a description of how a company is using and disclosing their personal information. This is a requirement under Gramm-Leach-Bliley's Financial Privacy Rule.

In the area of children's information, we have brought cases under the Children's Online Privacy Protection Act – – the law that requires parental consent prior to collecting information from children online. In some of these cases, the FTC has collected civil penalties for violating this law – and in the most recent case, $400,000 in civil penalties.

I could go on about our enforcement actions but I know that we have a full agenda, so I will move on to self-regulation and consumer and business education.

III. Self-regulation

Self-regulation also plays a role in the U.S. privacy framework, and businesses have taken steps to achieve meaningful self-regulation. For example, many companies participate in online privacy seal programs and adhere to industry codes of conduct. The goal is for self-regulation to be an efficient and effective partner in protecting

consumers from the harm that can result when their personal information is wrongfully obtained or misused.

IV. Consumer and Business Education

At the Federal Trade Commission, we strive to educate consumers and businesses about how to prevent harm before it happens. Last year, we distributed about 7 million print publications and logged over 20 million online accesses to our publications. Our products include brochures, compliance guides, bookmarks, one-page "news you can use" alerts, radio public service announcements, posters, postcards, websites, and newsletters. We are fortunate that Nat Wood, the Assistant Director at the FTC's Office of Consumer and Business Education is here today to demonstrate a recently launched web site, OnGuardOnline.gov. The FTC, other federal agencies (including the Department of Commerce), and the technology industry have teamed up to create this Web site to help computer users guard against Internet fraud, secure their computers, and protect their personal information. I am now pleased to introduce you to Nat Wood.