Remarks of Lydia B. Parnes[1]
Director, Bureau of Consumer Protection, Federal Trade Commission
The 16th Annual Conference on Computers, Freedom and Privacy
Washington, D.C.
May 4, 2006

I. Introduction

Good morning. I'm pleased to be here today for the 16th Annual Conference on Computers, Freedom, and Privacy. This is a dynamic and diverse group of people who care deeply about privacy, enjoy a robust debate, and are not afraid of controversy. Lawmakers, privacy advocates, academics, security experts, and even hackers come here to debate the most cutting-edge issues of the day. Where else can you enjoy a continental breakfast while watching Rob Atkinson, President of the Information Technology and Innovation Foundation face off with Katherine Albrecht, founder and director of CASPIAN, on RFID? I too enjoy a robust debate and I'm delighted to have the opportunity to speak with you today.

I am here this morning because consumer privacy and security are top priorities for the Federal Trade Commission. Chairman Majoras has placed these issues at the forefront of our consumer protection program and has invested the resources to back up that commitment. In 2006, Chairman Majoras established a new division, the Division of Privacy and Identity Protection, or "DPIP." This new division -- which consists of more than 30 staff members with expertise in privacy, data security, and identity theft -- addresses emerging consumer privacy matters through aggressive enforcement, as well as rulemaking, policy development, and outreach to consumers and businesses. To be sure, all eight divisions in our Bureau of Consumer Protection adeptly tackle privacy issues, but they also do other, critical consumer protection work. At DPIP, it is all privacy and security, all the time.

Like the impressive agenda for this four-day conference, the FTC's privacy program tackles a wide range of issues. We share CFP's concerns about consumers' privacy in the online world. This concern is reflected in our efforts to combat spam, phishing, spyware, Internet trickery, deceptive privacy policies, and poor security practices that place consumers' sensitive data at risk. But we are equally concerned about consumer privacy in the brick-and-mortar space. Our efforts on this front include the implementation of the National Do Not Call Registry, tough enforcement against pretexters and telemarketers, and campaigns to help protect sensitive data stored the old fashioned way – paper files. State-of-the-art computer security is critical, but so is the proper disposal of sensitive paper records. It doesn't help to have bulletproof encryption for credit card numbers transmitted over the Web if you toss out old sales data in public dumpsters.

Our focus, both in the online and offline contexts, is on consumers' personal, sensitive information. In today's information economy, consumer data is a valuable commodity – like cash – and it should be treated that way. We would not expect a bank to bolt shut the front door but leave the back door open. The front and back doors must be locked, the windows sealed, and the vault tightly shut. Companies – and consumers – must protect sensitive information in the same way. Companies must secure their back doors from tech savvy hackers, spyware and malware, and digital identity thieves. And they must keep data from waltzing out the front door as a result of accidental disclosure, improper disposal, poor training, pretexting, or good ol' fashioned theft.

With this "back door – front door" metaphor in mind, this morning I would like to focus on a trio of privacy issues: pretexting, spyware, and information security.

II. Pretexting

I am going to start with the front door – the most obvious exit for sensitive information – and perhaps the easiest to slam shut. Why break in through a window if you can just knock on the door and ask for the goods?

"Pretexting" is the practice of obtaining personal information, such as financial or telephone records, under false pretenses. It is not new. But it can cause substantial consumer injury. And it serves as a reminder that in the 21st Century, when the focus is on technology, we need to remain vigilant in our efforts to halt bread-and-butter data theft done the old fashioned way – lying.

Companies that engage in pretexting not only violate the law, but they undermine consumers' confidence in the marketplace and in the security of their sensitive data. Pretexting of phone call records in particular, has attracted substantial attention in recent months.[2] The Federal Trade Commission Act prohibits unfair and deceptive practices in commerce, and there is a long history of using it to challenge unfair and deceptive information collection practices.[3] In fact, as early as the 1960's, when the "welcome wagons" greeted new neighbors, we took action against a local credit bureau using the welcome wagon to deceptively collect information.[4]

The Commission filed its first modern pretexting suit in 1999 against a company that offered to provide consumers' bank account numbers and balances to anybody for a fee.[5] Later that year, Congress enacted the Gramm-Leach-Bliley Act, which expressly prohibits pretexting for financial records.[6] Since GLB's passage, the FTC has sent warning letters to 200 firms that sold asset information to third parties and brought more than a dozen financial pretexting cases.[7]

More recently, a cottage industry of companies offering to provide purchasers with phone records of third parties emerged. Although telephone records are protected by Federal law, these companies freely sell them to any buyer. This is a serious intrusion into consumers' privacy and can facilitate stalking, harassment, and worse.

Just yesterday, the FTC announced five law enforcement actions filed in federal district court against a dozen individuals and related corporate entities who allegedly engaged in the unauthorized sale of confidential customer phone records and, in one case, financial information.[8] In each case, we alleged that the defendants, or third parties with whom they contract, obtained the records through false pretenses, in some cases posing as a consumer to obtain the confidential and non-public personal information.

The defendants advertised over the Web that they could obtain confidential customer phone records from phone companies for a fee, offering to obtain details of incoming and outgoing phone records for any phone number. The complaints alleged that each defendant sold wireless and land line phone records, including lists of numbers called and the time, date, duration and, in some cases, originating location of calls. The FTC alleged that the invasion of privacy and security resulting from obtaining and selling confidential phone records without the consumers' authorization causes substantial injury to consumers and the public, including, but not limited to, endangering the health and safety of consumers. State attorneys general and cell phone providers have filed similar suits, and the Federal Communications Commission is taking steps to ensure that cell phone companies provide better protection for the records in the first place.[9]

These cases were in part a result of a petition filed by the Electronic Privacy Information

Center ("EPIC"). We appreciate the information provided to us in this petition.

In sum, companies must invest more resources to ensure that sensitive data does not walk out the front door. If employees understand the value of data and know the policies that are in place to safeguard that information, pretexting would be a scam of the past.

III. Data Security

Lets move from the front door to the back door. Here, hackers and cybercriminals of all shapes, sizes, and ability, use digital picks to break into companies' databases and abscond with treasure troves of sensitive data.

The growth of the Internet and the development of sophisticated computer systems and databases has made it easier than ever for companies to gather sensitive information about their customers, employees, and business associates. These information systems – online and off – play an increasingly important role in the global electronic marketplace. Make no mistake: there are enormous benefits to consumers from this new electronic commerce. But as the recent security breaches demonstrate, if data is not adequately secured, it can fall into the wrong hands. And, the consequences of security breaches often are severe, ranging from identity theft and unauthorized charges on consumers' accounts to an increase in spam and "phishing" schemes.

News reports about data breaches continue to break almost weekly. Just last week, the University of Texas at Austin announced that someone had broken into a computer at its McCombs School of Business and gained access to a database containing confidential information on about 200,000 people.[10] The breached database contained confidential information, including names, dates of birth and Social Security numbers. By one count, there have been over 150 incidents nationally since February 2005 in which the personal data of nearly

55 million consumers have been affected.[11]

The current state of affairs is not acceptable. But I don't need to lecture this group on dangers of computers and networks, or the hazards that lurk in the dark alleys of the Internet. You have been at the forefront of these issues for years. And so have we.

The FTC has an active law enforcement program to address data breaches and encourage appropriate security. The FTC has challenged unfair and deceptive security practices, as well as violations of the Fair Credit Reporting Act (FCRA)[12] and the Gramm-Leach-Bliley Act (GLBA).[13] Most of these cases focused on the company's failure to secure the back door into consumer data. Consider the FTC's three recent unfairness cases.[14] In each case, the FTC alleged that the companies engaged in a number of practices, *taken together*, that did not provide reasonable security for sensitive consumer information. In all three cases an unauthorized party obtained access to credit and debit card information. In other words, the companies were hacked – but not by the most sophisticated cybercriminals – these hackers exploited reasonably foreseeable security risks that the company should have taken steps to correct. The vulnerabilities we alleged were well-known within the information technology industry and simple, low cost measures were readily available to prevent them. The companies, however, left their digital doors open.

But again, I can't emphasize enough that the back door is not the only data security concern. Unless you've disconnected your PCs, blackberrys, cell phones, wireless devices and pagers for the past two months, then you have heard about the FTC's law enforcement action against consumer data broker ChoicePoint, Inc.[15] According to our complaint, ChoicePoint's security failures allowed identity thieves to obtain access to the personal information of over

160,000 consumers, including nearly 10,000 consumer reports, and to commit identity theft. The FTC alleged that ChoicePoint failed to use reasonable procedures to screen prospective subscribers in violation of the FCRA and the FTC Act.[16] For example, the company allegedly approved as customers individuals who lied about their credentials, used commercial mail drops as business addresses, and faxed multiple applications from nearby public commercial locations. In other words, they came in through the front door. The Commission obtained a record $10 million in civil penalties for the FCRA violations, $5 million in consumer redress for identity theft victims, and significant injunctive provisions.

The core principle underlying all of our security cases is that companies must implement reasonable and appropriate measures to protect sensitive information. This reasonable standard is the essence of the FTC's GLB Safeguards Rule which requires financial institutions to put in place safeguards for consumer data. But what does that mean? And how does it help? There's been a lot of discussion about this standard. Its main benefit is flexibility. It allows different types of companies – with different structures, sizes, ways of handling information – to implement security that works best for them. It also adapts to changes over time – changes in technology, changing threats to data security, changes in a company's way of doing business. The standard also distinctly recognizes that perfect security is unattainable, that companies can and should weigh the relative costs and benefits of implementing various security measures, and that there shouldn't be strict liability for a breach. In fact, the FTC has declined to take action against a number of companies that had breaches but had taken reasonable precautions.

The ultimate goal here is not to put another notch in our enforcement belt. Rather, it is to create a culture of security for sensitive information so that businesses prevent breaches and

identity theft. Simply put, companies must take information security seriously, integrate it into their day-to-day operations, and be proactive in identifying and addressing risks.

IV. Spyware

And now, I would like to turn to the third issue in my privacy trio: spyware. Spyware and other menacing software often provide digital data thieves with a back door into consumers' online lives. Again, no need to pontificate in this forum about the dangers posed by spyware. You get it. And we get it!

Spyware presents consumer protection issues similar to those posed by more traditional technologies. As with other frauds and scams, tough enforcement of existing consumer protection laws is an important step to prevent the spread of spyware. Using the FTC Act's grant of broad authority to challenge unfair or deceptive acts and practices, the Commission launched an aggressive law enforcement program to fight spyware. To be sure, spyware presents serious new challenges in detection, apprehension, and enforcement. But through litigation, the FTC has successfully challenged the distribution of spyware that causes injury to consumers in the online marketplace.

Our spyware law enforcement program is guided by three key principals, which apply not only to spyware, but to adware, malware, and other unwanted software. First, a consumer's computer belongs to him or her, not software distributors. The consumer must agree to have software installed, not be tricked into it.

Second, buried disclosures do not work with software, just like they have never worked in other areas of commerce. In other words, burying critical information in the End User License Agreement, or EULA, does not satisfy the well established requirements for clear and

conspicuous disclosure.

And third, if a distributor places unwanted software on a consumer's computer, the consumer must be able to uninstall or disable it.

This morning, let me highlight just one case, FTC v. Seismic Entertainment.[17] This case illustrates the first principle – the basic common-sense notion that the resources of a consumer's computer are his or her own, and Internet businesses can not use these resources without the consumer's permission. In Seismic, we alleged that the defendants exploited known vulnerabilities in Internet Explorer to download spyware to consumers' computers without their knowledge. This spyware, among other things, hijacked consumers' home pages, caused the display of an incessant stream of pop-up ads, allowed the secret installation of additional software programs, and caused computers to severely slow down or crash. The FTC alleged that defendants' use of "drive-by" tactics to download spyware was unfair in violation of Section 5 of the FTC Act.

The Seismic case is not just about principles. It is about tough enforcement. This morning, the FTC announced that we obtained a $4.1 million judgment against the primary defendants in Seismic – Sanford Wallace and his company SmartBot.Net, Inc.[18] The final order also prohibits them from downloading software in the future without consumer authorization. Our staff also obtained a $330,000 judgment against a second group of defendants who allegedly assisted Wallace in his distribution of spyware. This $330,000 represents the full amount that they earned from the scheme. This $4.5 in judgments is an important victory for consumers and also an important lesson for those who would exploit advancements in technology for their

financial gain.

I have highlighted just one of our cases this morning. To date, we have filed six spyware and adware cases and are aggressively investigating others.[19] Over time, as technology changes and the methods used to distribute software evolve, these same three principles will remain relevant, whether, for example, software is downloaded from a CD-ROM, onto a mobile device, or through instant messaging. And backing up these principles will be tough enforcement.

V. The Next Tech-Ade

I have just presented a brief overview of how the FTC addresses some of today's most challenging high-tech consumer protection issues. But what about the issues of tomorrow? This November, the FTC will bring together experts from the business, government, and technology sectors, as well as consumer advocates, academics, and law enforcement officials to explore the ways in which convergence and the globalization of commerce impact consumer protection.[20] The upcoming hearings will examine changes that have occurred in marketing and technology over the past decade, and garner experts' views on emerging challenges and opportunities for consumers, businesses, and government. I would encourage each of you to participate this fall – and yes, even the hackers in the room are welcome.

VI. Conclusion

I could go on... and on ... and on. I think you get my message: Companies and consumers must take information security seriously and make sure that information does not walk out the front door and is not stolen out the back door. And I can assure you, that as we go forward, and face new technologies and new challenges, privacy protection efforts will continue to occupy a central role in our consumer protection mission.

I really appreciate you asking me to be here today, and if we have time, I would be happy to take any questions.

1. The views expressed herein are my own and do not necessarily represent the views of the Federal Trade Commission or of any Commissioner.

2. For example, recent news stories state that reporters obtained cell phone records of General Wesley Clark and cell phone and land line records of Canada's Privacy Commissioner Jennifer Stoddart. *See, e.g.*, Aamer Madhani and Liam Ford, *Brokers of Phone Records Targeted*, Chicago Trib., Jan. 21, 2006, *available at* 2006 WLNR 1167949.

3. 15 U.S.C. § 45. An act or practice is unfair if it: (1) causes or is likely to cause consumers substantial injury; (2) the injury is not reasonably avoidable by consumers; and (3) the injury is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

4. *In the Matter of The Credit Bureau of Washington, D.C.*, FTC Docket No. C-2113 (Dec. 7, 1971)(consent order challenged operation of new resident information-reporting service under the name Welcome Newcomer that used deceptive practices to collect personal and financial information from new area residents).

5. *FTC v. James J. Rapp and Regana L. Rapp, d/b/a Touch Tone Information, Inc.*, No. 99-WM-783 (D. Colo.) (final judgment entered June 22, 2000). *See* http://www.ftc.gov/os/2000/06/touchtoneorder.

6. 15 U.S.C.§§ 6801-09.

7. *See, e.g*, FTC press release "As Part of Operation Detect Pretext, FTC Sues to Halt Pretexting" (Apr. 18, 2001), *available at* http://www.ftc.gov/opa/2001/04/pretext.htm. *See also FTC v. Victor L. Guzzetta, d/b/a Smart Data Systems*, No. CV-01-2335 (E.D.N.Y.) (final judgment entered Feb. 25, 2002); *FTC v. Information Search, Inc., and David Kacala*, No. AMD-01-1121 (D. Md.) (final judgment entered Mar. 15, 2002); *FTC v. Paula L. Garrett, d/b/a Discreet Data Systems*, No. H 01-1255 (S.D. Tex.) (final judgment entered Mar. 25, 2002). For more information about the cases the Commission has brought under Section 521 of the GLBA, *see* http://www.ftc.gov/privacy/privacyinitiatives/pretexting_enf.

8. *See* FTC press release "FTC Seeks Halt to Sale of Consumers' Confidential Telephone Records" (May 3, 2006) *available at* http://www.ftc.gov/opa/2006/05/phonerecords.htm.

9. For example, the Attorneys General of Florida, Illinois, and Missouri recently sued companies allegedly engaged in pretexting. *See* http://myfloridalegal.com/__852562220065EE67.nsf/0/D510D79C5EDFB4B98525710000Open&Highlight=0,telephone,records; http://www.ag.state.il.us/pressroom/2006_01/20060120.html; http://www.ago.mo.gov/newsreleases/2006/012006b.html. Several telecommunications carriers also have sued companies that reportedly sell consumers' phone records. According to press

reports, Cingular Wireless, Sprint Nextel, T-Mobile, and Verizon Wireless have sued such companies. *See, e.g.*, http://www.upi.com/Hi-Tech/view.php?StoryID=20060124-011904-6403r; http://www.wired.com/news/technology/1,70027-0.html; http://news.zdnet.com/2100-1035_22-6031204.html.

10. *See* press release "Unauthorized access of computer records discovered at The University of Texas at Austin" (April 23, 2006) *available at* http://www.utexas.edu/opa/news/2006/04/data23.html

11. *See* Privacy Rights Clearinghouse "A Chronology of Data Breaches Reported Since the ChoicePoint Incident" *available at* http://www.privacyrights.org/ar/ChronDataBreaches.htm

12. 15 U.S.C. §§ 1681-1681x.

13. 15 U.S.C. § 6801(b); Standards for Safeguarding Customer Information, 16 C.F.R. Part 314 ("Safeguards Rule"), *available at* http://www.ftc.gov/os/2002/05/67fr36585.pdf.

14. *In the Matter of DSW, Inc.*, FTC Docket No. C-4157 (Mar. 7, 2006); *In the Matter of CardSystems Solutions, Inc.*, FTC Docket No. 052-3148 (proposed settlement posted for public comment on Feb. 23, 2006); *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005).

15. *United States v. ChoicePoint*, Inc., No. 106-CV-0198 (N.D. Ga. Feb. 15, 2006).

16. The FTC issued a four count complaint against ChoicePoint: Counts I and II alleged violations of the FCRA, Count III alleged that ChoicePoint engaged in unfair practices in violation of Section 5 of the FTC Act, and Count IV alleged that ChoicePoint engaged in deceptive acts or practices in violation of Section 5 of the FTC Act. *United States v. ChoicePoint*, Inc., No. 106-CV-0198 (N.D. Ga. Feb. 15, 2006).

17. *FTC v. Seismic Entertainment, Inc.*, No. 04-377-JD, 2004 U.S. Dist. LEXIS 22788 (D.N.H. Oct. 21, 2004).

18. *See* FTC press release "Courts Halt Spyware Operations" (May 4, 2006) *available at* http://www.ftc.gov/opa/2006/05/seismic.htm.

19. *See FTC v. MaxTheater, Inc. et al*, No. 05-CV-0069 (E.D. Wash. March 8, 2005); *FTC v. Trustsoft, Inc., et al.*, Civ. No. H 05 1905 (S.D. Tex May 31, 2005); *FTC v. Seismic Entertainment, Inc., et al.*, No. 04-377-JD, 2004 U.S. Dist. LEXIS 22788 (D.N.H. Oct. 21, 2004); *FTC v. Enternet Media, et al.*, CV 05-7777 CAS (C.D. Cal., Nov. 1, 2005); *In the Matter of Advertising.com*, FTC File No. 042 3196 (Sept. 12, 2005); and *FTC v. Odysseus Marketing, Inc.*, No. 05-CV-330 (D.N.H. Sept. 21, 2005).

20. *See* FTC press release "FTC to Host Global Marketplace Hearings" (Feb. 9, 2006), *available at* http://www.ftc.gov/opa/2006/02/globalmarketing.htm.