Remarks of Lydia B. Parnes[1]
Acting Director, Bureau of Consumer Protection, Federal Trade Commission
Before the International Association of Privacy Professionals
Washington, D.C.

March 10, 2005

I. INTRODUCTION

Good morning. It is a pleasure to be here again and to see so many familiar faces, especially at 8:15 a.m. Privacy is increasingly becoming a global issue and I am delighted that joining us this morning are the Data Protection Commissioners from the Netherlands, Argentina, and Ireland. Although our approaches may be different, our objectives are the same – to protect the privacy of our citizens. I am looking forward to their remarks this morning.

Last October, I had the opportunity to speak to the IAPP Summit in New Orleans.[2] At that time, although Chairman Majoras was just three months into her tenure at the FTC, protecting consumer privacy was already high on her agenda. As the Chairman has more fully developed her priorities for the FTC, I am pleased to report that privacy and information security continue to be at the forefront of our consumer protection program.

In the still-young twenty-first century, technology continues to redefine how information is collected and used. The focus of the FTC's privacy program is to ensure that companies honor their privacy promises and that the information they collect is not misused in a way that harms consumers. Our goal is to strike the right balance between the many benefits the information-

---

[1] The views expressed are those of Lydia Parnes and do not necessarily reflect the views of the Commission or of any individual Commissioner.

[2] S*ee The FTC and Consumer Privacy: Onward and Upward*, available at http://www.ftc.gov/speeches/parnes/041028conprivparnes.pdf .

based economy provides to consumers and the potential harm that can be caused by the misuse of consumers' personal information.

Recent news reports about the release of consumers' sensitive information from one of the nation's largest commercial information services and a major U.S. bank underscore the importance of protecting consumers' personal information. Simply stated, this is extraordinarily valuable information and these security breaches are unacceptable. I will share more about our specific information security cases with you in a moment. But first, I would like to emphasize the message that the FTC has been promoting for several years: Companies must implement reasonable and appropriate measures to protect consumers' information. Our primary goal is to encourage all companies to put in place solid information security practices *before* a breach can occur. But where significant breaches do occur, we will continue to determine whether they were caused by the failure to take reasonable steps to safeguard consumers' information.

We are devoting significant resources to implement our privacy program and now I would like to share with you some of our recent initiatives.

II. PRIVACY LAW ENFORCEMENT IN THE 21st CENTURY

At the center of our privacy program is aggressive law enforcement. Privacy and American Business, a project of the Center for Social and Legal Research, tracks consumer privacy litigation – that is – suits alleging violations of consumer privacy rights by businesses. It recently reported that the FTC accounts for almost one-third of new privacy cases tracked in 2004. It also predicted that the FTC will be one of the key "litigation starters" in 2005 in the area of consumer privacy. We take this as a compliment, and we intend to prove them right. Our privacy law enforcement efforts focus on: (1) information security and information sharing;

(2) spam; (3) spyware; and (4) telemarketing.

A. Privacy and Information Security Enforcement

Over the last four months, the Commission continued its law enforcement efforts to prosecute companies that misrepresent their privacy policies. The agency gives special emphasis to representations concerning the *security* provided for customer information. To quote Chairman Majoras, "nothing today is more fundamental to privacy than information security."

The explosive growth of the Internet and the development of sophisticated computer systems and databases has made it easier than ever for companies to gather and use information about their customers, employees, and business associates. Information systems – online and offline – collect and store volumes of data on consumers and play an increasingly important role in the global marketplace. As the recent security breaches demonstrate, if this data is not adequately secured, it can fall into the wrong hands and cause serious harm to consumers. The consequences of security breaches are often severe, ranging from identity theft and unauthorized charges to consumers' accounts, to an increase in spam and "phishing" schemes.

Due to the importance of information security to consumers, this agency has made it one its top law enforcement priorities, and we will be dedicating even more resources to this critical issue. Our efforts in this area focus on false claims about security practices and failure to comply with the security requirements of the Gramm-Leach-Bliley Act ("GLBA"). To date, we have filed five cases challenging false security claims under Section 5 of the FTC Act.[3] In each

---

[3] *Petco Animal Supplies, Inc.* (Docket No. C-4133); *MTS Inc., d/b/a Tower Records/Books/Video* (Docket No. C-4110); *Guess?, Inc.* (Docket No. C-4091); *Microsoft Corp.* (Docket No. C-4069); *Eli Lilly & Co.* (Docket No. C-4047). Documents related to these enforcement actions are available at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.

case, we alleged that the companies involved promised that they would take reasonable steps to protect consumers' sensitive information, but failed to do so.

Last week, the Commission finalized the settlement of the fifth case.[4] The FTC alleged that Petco Animal Supplies promised to keep its customers' information secure, but failed to take reasonable measures to prevent commonly known attacks to its Web site by hackers. The flaws in Petco's Web site allowed a hacker to access consumer records, including credit card numbers. As with the Commission's prior information security cases, the settlement requires that Petco implement a comprehensive information security program for its Web site. Our message: consumers have the right to expect companies to keep their promises about the security of the confidential consumer information they collect.

The Commission also recently announced its first cases enforcing the Gramm-Leach-Bliley Safeguards Rule, which requires financial institutions to have reasonable procedures to ensure the security of customer information.[5] As part of a nationwide compliance sweep, the FTC charged two mortgage companies with violating the Rule.[6] The FTC alleged that the brokers failed to implement required safeguards to protect customer names, Social Security numbers, bank account numbers, and other sensitive financial information. The settlements bar future violations of the Rule and require independent audits of the companies' security programs. More investigations of Safeguards Rule violations are underway.

---

[4] *Petco Animal Supplies, Inc.* (Docket No. C-4133)(final consent order approved March 4, 2005).

[5] 15 U.S.C. § 6801(b); Standards for Safeguarding Customer Information, 16 C.F.R. Part 314 ("Safeguards Rule").

[6] *Sunbelt Lending Services*, (Docket No. C-4129) (consent order); *Nationwide Mortgage Group, Inc.*, (Docket No. 9319) (consent order)((Placed on the public record on March 4, 2005).

Although the FTC emphasizes information security, we are also concerned about companies' policies for disclosing information to third parties. Today, we are announcing another case challenging a company's information sharing practices.[7] In this case, the FTC alleged that CartManager International, a company that provided shopping cart services to thousands of online merchants, collected and shared the personal information of merchants' customers knowing that such practices were contrary to merchant privacy policies. According to our complaint, CartManager shared the personal information of nearly one million consumers for rental to third parties for marketing. Companies and service providers need to make sure that their information practices and policies are in synch. A service provider cannot surreptitiously collect and use consumers' personal information for its own gain and in ways contrary to a merchant's privacy policy.

B. Spam Enforcement

Spam remains a serious consumer privacy problem. One study released just two weeks ago estimates that spam will cost the world $50 billion in lost productivity and other expenses, with more than a third of that – $17 billion – wasted by U.S. firms.[8] At the FTC, we are continuing to attack spam on multiple fronts, including using aggressive law enforcement to stop the worst perpetrators.

To date, we've filed 68 spam-related cases against 198 individuals and companies. In one recent case, the FTC filed suit against a network of individuals and corporations that used

---

[7] *In the Matter of Vision I Properties, LLC, doing business as CartManager International*, FTC File No. 042-3068 (consent order) (Placed on the public record on March 10, 2005).

[8] Ferris Research, *The Global Economic Impact of Spam*, 2005 Report, released February 2005.

spam to sell access to online pornography.[9] The Commission alleged that the defendants barraged consumers with sexually explicit email that violated virtually every provision of the CAN-SPAM Act, including the Adult Labeling Rule. The court immediately issued a temporary restraining order and has since entered a preliminary injunction. This may be our first case enforcing the Adult Labeling Rule, but it is far from our last.

Working with criminal law enforcers remains a priority for the FTC. The FTC's Criminal Liaison Unit, or CLU, continues to enhance the Commission's working partnerships with various criminal law enforcers so that scammers do not evade criminal sanctions. This is particularly important for our CAN-SPAM enforcement program. We continue to strengthen relationships with various U.S. Attorney Offices, the Postal Inspection Service, and the Department of Justice. In addition, through CLU's efforts, Justice Department staff regularly visit the FTC Internet Lab to search our state-of-the-art spam database and identify new targets for prosecution.

Of course, spam is a technological problem, and the solution must include technological fixes. Last November, the Commission convened an Email Authentication Summit, co-sponsored by the National Institute of Standards at the Commerce Department.[10] Since the Summit, the FTC has been encouraging the development of a compatible authentication standard that will provide accountability for email communication.

Spam does not just threaten consumers' privacy, it threatens confidence in the Internet as

---

[9] *FTC v. Global Net Solutions, Inc.*, No. CV-S-05-0002-PMP-LRL (D. Nev. filed Jan. 3, 2005).

[10] *See* www.ftc.gov/bcp/workshops/e-authentication/index.htm.

a medium for commerce and communication. Therefore, as long as you find spam in your inbox, you'll find the FTC on the spam beat. We will continue to emphasize CAN-SPAM enforcement and work with our criminal law enforcement partners to put the worst offenders behind bars. The stakes are high, and all involved have an interest in ensuring the continuing viability of email communications.

C. Spyware Enforcement

After spam, spyware is becoming one of the most serious consumer problems on the Internet. To address the adverse effects of this digital menace, the FTC is investigating and aggressively prosecuting spyware distributors.

In September 2004, the FTC filed its first case challenging the distribution of spyware as a violation of the FTC Act.[11] The FTC alleged that the defendants downloaded spyware that surreptitiously changed consumers' home pages, triggered a barrage of pop-up ads, and even installed additional software that can track a consumer's computer use. The court enjoined the defendants' unlawful practices and a trial is scheduled for this November.

We are also targeting the deceptive marketing of purported "anti-spyware" software products. Consumers are being duped into buying useless software by scam artists looking for a quick buck. The dissemination of useless anti-spyware products leaves consumers vulnerable to spyware, although they think they are adequately protected. Such deceptive practices in the online marketplace, which exacerbate the growing threat of spyware, will not be tolerated. Our first case targeting this deceptive conduct will be announced in the very near future.

While these cases are difficult to investigate and prosecute, we are giving them a high

---

[11] *FTC v. Seismic Entm't Productions, Inc.*, No. 04-377-JD (D.N.H. filed Oct. 6, 2004).

priority.

D. Enforcement of the National Do Not Call Registry

The National Do Not Call Registry protects consumer privacy by prohibiting calls to consumers who register their telephone numbers on the list. As of March 1, 2005, consumers had registered more than 84 million telephone numbers. Compliance with this new law has been very high and we intend to keep it that way.

Since October 2003, the Commission filed five enforcement actions alleging that the defendants called consumers whose numbers were on the Registry, and it has forwarded two additional cases to the Department of Justice for filing.[12]

Last month, the Commission announced settlements in the first strictly civil penalty Do Not Call enforcement actions.[13] Under the final orders, two timeshare sellers agreed to pay $500,000 in civil penalties and abide by a federal court injunction. The telemarketers they retained were banned from owning or operating a telemarketing operation and agreed to a suspended judgment of over $526,000. According to the complaints, these defendants repeatedly violated the Registry provisions of the FTC's Telemarketing Sales Rule, failed to pay the fees required to access the Registry, and unlawfully abandoned calls to consumers.

III. EVALUATING THE IMPACT OF 21ST CENTURY TECHNOLOGY ON

---

[12] *FTC v. Nat'l Consumer Council*, No. SACV 04-0474 CJC (JWJx) (C.D. Cal. filed Apr. 23, 2004); *FTC v. Internet Mktg. Group*, No. 3-04 0568 (M.D. Tenn. filed June 29, 2004); *FTC v. Debt Mgmt. Found. Services, Inc.*l, No. 8:04-CIV-1674-T-17-MSS (M.D. Fla. filed July 20, 2004); *United States v. Braglia Mktg. Group, LLC*, No. CV-S-04-1209-DWH-PAL (D. Nev. filed Aug. 20, 2004); *FTC v. 3R Bancorp,* No. 04C-7177 (N.D. Ill. filed Nov. 5, 2004); *United States v. Flagship Resort Development Corp.*, No. 05-CV-981 (D. N.J. filed February 16, 2005).

[13] *United States v. Braglia Mktg. Group, LLC*, No. CV-S-04-1209-DWH-PAL (D. Nev. filed Aug. 20, 2004); *United States v. Flagship Resort Development Corp.*, No. No. 05-CV-981 (D. N.J. filed February 16, 2005).

CONSUMERS

Our law enforcement program is complemented – and informed by – our efforts to explore the impact of new technology on consumer privacy. New technologies are radically changing the contours of the twenty-first century marketplace. Through research, studies, and workshops, we endeavor to understand the benefits and risks posed by these new technologies, and to examine various self-regulatory and technological efforts to address consumer concerns. These efforts also help the FTC identify the most egregious fraud, deception, and rule violations for law enforcement or other action.

A. Radio Frequency Identification

Radio frequency identification, or RFID, is one of the technologies the FTC is exploring. Although not new, RFID is now being used in novel ways, and its use is expected to grow as the technology's capabilities are improved. As with other emerging information technologies, RFID has great potential benefits. However, it also poses potential risks to consumer privacy.

Last year, the Commission convened a public forum to explore the benefits and concerns associated with RFID and on Tuesday we released a staff report summarizing the workshop discussions and offering some conclusions from Commission staff.[14] As with the general technology itself, the core principles underlying the staff's recommendations are not new. First, industry initiatives can play an important role in addressing privacy concerns raised by certain RFID applications. The goal of such programs should be transparency. For example, companies should clearly and conspicuously disclose to consumers when and how they use RFID

[14] RFID: Radio Frequency IDentification: Applications and Implications for Consumers: A Workshop Report From the Staff of the Federal Trade Commission, available at http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf

technology. Similarly, if a company's program provides consumers with the option of removing the RFID tag, the company's practices should make that option easy to exercise by consumers. Second, many of the potential privacy issues associated with RFID are inextricably linked to information security. As I discussed earlier, a company that collects consumers' sensitive information, through RFID or any other technology, must implement reasonable and appropriate measures to protect that data. Third, consumer education is a vital part of protecting consumer privacy. Industry members, privacy advocates, and government should develop education tools that inform consumers about RFID technology.

RFID is a rapidly-evolving technology. As new applications emerge, we will consider what additional guidance or other actions are appropriate.

B. Spyware

Last year, the FTC also held a public workshop to learn more about spyware.[15] The workshop provided information to the Commission and other government officials to guide and focus our legislative, regulatory, law enforcement, and consumer education efforts. It also elicited important information concerning whether market forces, technological innovation, self-regulation, and other industry efforts could mitigate the problems associated with spyware.

On Monday, we released our staff workshop report.[16] Like the speakers on the spyware panel at the IAPP Summit last October, the FTC staff concluded that it is difficult to define spyware with precision. Despite the absence of a clear definition, however, it is clear that

---

[15] Transcripts from the public workshop, *Monitoring Software on Your PC: Spyware, Adware, and Other Software*, are available at <www.ftc.gov/bcp/workshops/spyware>.

[16] Monitoring Software on Your PC: Spyware, Adware, and Other Software, available at http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf

spyware is a real and growing problem. The issue: how do we solve that problem?

Staff concluded that spyware *can* be decreased if *both* the private sector and the government act. First, technological solutions like firewalls, anti-spyware software, and improved browsers and operating systems can provide significant protection to consumers from the risks related to spyware. Second, industry should develop standards for defining spyware and disclosing information about it to consumers; expand efforts to educate consumers about spyware risks; and help law enforcement efforts. And for its part, government should increase criminal and civil prosecution of those who distribute spyware; beef up efforts to educate consumers about the risks of spyware; and encourage technological solutions.

C. The FACT Act

Our research, reports, and studies extend beyond emerging technologies. The FTC also focuses on the most intractable consumer protection problems. One of the most pressing problems is Identity Theft.

The Fair and Accurate Credit Transactions Act of 2003 (the FACT Act) provides important tools to help prevent identity theft and assist identity theft victims.[17] The FACT Act requires the FTC, alone or in conjunction with other agencies, to adopt 18 rules, undertake eight studies, and conduct three consumer education campaigns. Last year, the FTC completed 10 FACT Act rules, proposed three additional rules, and published five studies. These rules and studies highlight the critical importance of the goal of our privacy program – striking just the right balance between the benefits that an information society can provide to consumers, and the severe consequences that can result when consumer information is misused.

---

[17] On December 4, 2003, the Fair and Accurate Credit Transactions Act of 2003 ("FACTA") was enacted. Pub. L. No. 108-159 (2003) (codified at 15 U.S.C. § 1681 *et seq.*). Many of the provisions amend the Fair Credit Reporting Act. 15 U.S.C. § 1681 *et seq.*

IV. 21ST CENTURY PROBLEMS REQUIRE GLOBAL SOLUTIONS

Globalization is one of the central consumer protection developments of the twenty-first century, commanding the attention of businesses, consumers, law enforcers, and policymakers around the world. This is certainly true in the privacy arena where information is crossing borders faster than ever before. Similarly, telemarketing and Internet activities such as spam and spyware are not dependent on geography. The agenda for this conference confirms that consumer privacy is indeed a global issue.

Indeed, Chairman Majoras is placing an even greater emphasis on international consumer protection efforts. With regard to enforcement, many of the cases that we investigate include some cross-border element. The FTC has strong relationships with its counterparts in other countries, and we provide assistance to one another in the investigation and prosecution of cases. For example, in October, the FTC joined forces with agencies around the world to combat spam on a global level. This initiative, the London Action Plan, involves 26 agencies from 19 countries as well as some private sector participants.[18] The London Action Plan calls for increased investigative training and the creation of an international working group on spam enforcement.

This year, the FTC signed two bilateral memoranda of understanding with foreign law enforcement partners: one with Mexico's consumer protection agency to promote enhanced cooperation in the fight against cross-border fraud[19] and one with Spain's data protection agency

---

[18] *See* London Action Plan on International Spam Enforcement Cooperation, available at http://www.ftc.gov/os/2004/10/041012londonactionplan.pdf .

[19] The text of the Memorandum of Understanding On Mutual Assistance In Consumer Protection Matters Between the Federal Trade Commission of the United States of America and the Procuraduria Federal Del Consumidor (Office of the Federal Attorney for Consumer Protection) of the United Mexican States is available at

on spam enforcement.[20]

In addition, the FTC remains active in international policy issues relating to privacy. Just last month, I had the pleasure of meeting with Peter Schaar, Chairman of the European Article 29 Working Party. We discussed the Safe Harbor framework and its importance in this global economy. We also discussed privacy enforcement and the common goals shared by the United States and Europe. As I said earlier, although our particular approaches are different, we do share the common goal of privacy protection.

Finally, the Commission's highest legislative priority during the coming year is passage of the International Consumer Protection Act. This legislation will enhance our ability to pursue joint investigations with our international counterparts, including investigations into cross-border fraud and deception, spam, and spyware.

V. INFORMATION SECURITY – THE CRITICAL CONSUMER PROTECTION CHALLENGE FOR THE 21ST CENTURY

I would like to end where we started – information security. Although from a policy development standpoint we often discuss online security as discrete topics – hacking, viruses, spam, and spyware – the bottom line is that consumers just want to be able to surf the Internet safely. Even my tech-savvy colleagues have a difficult time keeping up-to-date on the latest spyware blockers, spam filters, anti-virus protection, firewalls, security settings, and software patches. Thus, a critical challenge for the 21st Century Internet age is making the process simpler for average users.

---

http://www.ftc.gov/os/2005/01/050127memounderstanding.pdf .

[20] The text of the Memorandum of Understanding On Mutual Enforcement Assistance In Commercial Email Matters Between the Federal Trade Commission of the United States of America and the Agencia Espanola de Proteccion de Datos is available at http://www.ftc.gov/os/2005/02/050224memounderstanding.pdf .

One can argue that consumers should take responsibility for their own computer safety. But we know from experience that if the process is difficult and requires "technological know how," security will be ignored – until it is too late. Chairman Majoras recently summed it up this way: "Given that we all have a tremendous stake in the security of – and consumer confidence in – the online world, it seems that making the world safer should be a priority for all stakeholders." Making the online world safer likely will require the deployment of user-friendly security features and security protections.

Thank you again for the opportunity to speak to you today about the FTC's multifaceted privacy program. I would be happy to take questions from the audience.