Remarks of Lydia Parnes*

Acting Director, Bureau of Consumer Protection

Before the IAPP

October 28, 2004

The FTC and Consumer Privacy:

Onward and Upward

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

It's a pleasure to be here. For more than a decade, the Federal Trade Commission has made privacy and data security a central part of its mission. More recently, as many of you know, there have been changes at the Commission. Chairman Deborah Platt Majoras took over the helm in August and I'm honored to serve as her Acting Bureau Director. My message today is simple: under Chairman Majoras, privacy and information security continues to be a top priority in the FTC's consumer protection program. The FTC's privacy program will continue to focus on the same core issues emphasized by our predecessors Tim Muris and Howard Beales: ensuring that companies honor their privacy promises and that the information they collect is not misused in a way that harms consumers. Our goals also remain the same: striking the right balance between the many benefits the information-based economy provides to consumers and the potential harm that can be caused by the misuse of consumers' personal information.

Today, I want to update you on where we are on that program and highlight our priorities for the next year. The "familiar faces" on the agenda are: implementing the National Do Not Call Registry; combating unwanted spam; promoting information security; enforcing privacy promises; and controlling identity theft. Our new challenges include radio frequency identification, peer-to-peer file sharing, and spyware. This is an exciting, active program.

THE NATIONAL DO NOT CALL REGISTRY

I've been at the FTC a long time, and during that time, the Commission has accomplished many things for consumers. But I have to say, I view the National Do Not Call Registry as our most notable consumer protection triumph. Whenever I ask groups like this whether any of the people in the audience are on the National Do Not Call Registry, and whether as a result they receive fewer telemarketing calls, the response is overwhelmingly "yes" on both counts. This is

consistent with what we are hearing from consumers across the country. Fewer Americans are now being interrupted by unwanted and intrusive telemarketing calls.[1]

We've come a long way since the Commission first proposed a national Do Not Call Registry. As of October 1, consumers registered approximately 64.4 million telephone numbers. Approximately 80,000 telemarketers are scrubbing their lists using our database.

Overall compliance with the Registry is outstanding. Although compliance is high, it is not perfect. Enforcement is a key part of our Do Not Call program. To date, we have filed four cases alleging Do Not Call violations.[2] In one recent case, we alleged that the company not only made calls to telephone numbers that were on the National Do Not Call Registry, but masqueraded as a non-profit in an attempt to skirt the Rule's requirements.[3] We charged the defendants with several law violations, including an allegation that the defendants falsely represented that they were a charity.

This case involves a combination of Do Not Call violations and other deceptive or fraudulent practices. However, you can run afoul of the Do Not Call Registry even without violating other laws. Our first civil penalty case for Do Not Call violations was filed last

---

[1]A Harris Interactive poll found that 92 percent of the respondents have received fewer telemarketing calls since they registered. Indeed, 25 percent say they are not getting any telemarketing calls at all since registering. *See* <http://www.harrisinteractive.com/harris_poll/index.asp?PID=400>.

[2]*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).

[3]*FTC v. Debt Mgmt. Found. Services, Inc.*, No. 8:04-CIV-1674-T-17-MSS (M.D. Fla. filed July 20, 2004).

August.[4] What got the telemarketers in trouble was not their sales pitch, but the fact that they made more than 300,000 calls to consumers who had put their phone numbers on the Registry. The FTC is authorized to obtain up to $11,000 per violation.

To sum it all up: we intend to use every tool in our legal tool box to vigorously and swiftly enforce the Do Not Call Registry.

SPAM

Controlling unwanted spam is one of the most daunting consumer protection issues that we face. The harm caused by this digital menace reaches far beyond mere annoyance or inconvenience. Spam indiscriminately spreads deceptive messages and sexually explicit material. Spam also creates serious security issues when it is used to transmit viruses, bugs, and worms. The sheer volume of spam threatens the utility of the email system itself. Finally, the constant barrage of often offensive spam undermines consumers' sense of privacy and security in the Internet.

Unfortunately, although it is easy to identify spam as a problem, it is not so easy to identify solutions. Spammers use a variety of techniques to anonymously send millions of email messages across the globe, hiding their identities and the origin of their email. To address spam, we are continuing our three-prong strategy: (1) law enforcement; (2) education; and (3) research.

First, law enforcement. We've filed 63 spam-related cases against 164 individuals and companies. Recently, we received our first written opinion enforcing the CAN-SPAM Act.[5] In

---

[4]*United States v. Braglia Mktg. Group, LLC*, No. CV-S-04-1209-DWH-PAL (D. Nev. filed Aug. 20, 2004).

[5]15 U.S.C. § 7701 *et seq.*

the *Phoenix Avatar* case, the Commission alleged that the defendants falsified header information and failed to offer consumers the ability to opt-out of receiving future email.[6] Importantly, the court held that "Liability is not limited to those who physically cause spam to be transmitted, but also extends to those who 'procure the origination' of offending spam." The message is: even if you didn't push the "send button" – if you profit from illegal spam, you may be liable for violations of the CAN-SPAM Act.

High-tech cases require high-tech tools. One of these tools is the FTC's spam database. This searchable database currently holds over 150 million pieces of spam that were forwarded to the FTC by consumers. And we are receiving approximately 300,000 new spam messages every day. Yes, we want your spam and you can forward it to spam@uce.gov. We use this database to build cases such as *Phoenix Avatar*. This summer, we provided several of our law enforcement partners with direct access to the database right from their desktops. By expanding access to the database, we're providing our partners with additional resources to combat spam.

But law enforcement alone will not solve the spam problem. A key part of our spam program is educating both consumers and businesses about self-help measures they can take against spam. We have a spam home page with links to publications for consumers and businesses.[7]

---

[6] *FTC v. Phoenix Avatar, LLC, et al.*, Case No. 04C 2897 (N.D. Ill. filed Apr. 23, 2004).

[7] The home page is located at <www.ftc.gov/spam>.

Research is the third prong of our spam program. Studies like our False Claims In Spam report[8] and our "remove me"surf[9] help us build better cases, develop timely education campaigns, and allocate our limited spam-fighting resources. Research also helps us fill the gaps in reliable information about email and separate the "spam facts" from the "spam fiction."

Most importantly, we are hoping to encourage the development of technological fixes for the spam problem. In two weeks, the FTC, together with the National Institute of Standards and Technology, will host a two-day Email Authentication Summit in Washington, D.C.[10] The genesis of the Summit was the Commission's Report to Congress on a proposed National Do Not Email Registry.[11] That Report recommended against the implementation of a Do Not Spam Registry. The Commission concluded that a Registry would not reduce the volume of spam and even has the potential to increase the amount of spam. Most spammers appear to care little about complying with the law. Why? Because spammers operate under a cloak of anonymity. To reduce unwanted spam, this cloak must be removed and enforcement made more certain. The Summit will explore the best way to do just that.

---

[8]*False Claims In Spam: A Report by the FTC's Division of Marketing Practices*, was issued on April 30, 2003. *See* <*www.ftc.gov/reports/spam/030429spamreport.pdf*>.

[9]A fact sheet illustrating the results of the "remove me" surf is available at <www.ftc.gov/bcp/conline/edcams/spam/pubs/removeme.pdf>.

[10]The agenda and public comments filed in response to the FTC's Request for Comments is available at <www.ftc.gov/bcp/workshops/e-authentication>. A transcript of the panels will be available after the Summit.

[11]*See* Federal Trade Commission, *National Do Not Email Registry: A Report to Congress* (June 2004), *available at* <http://www.ftc.gov/reports/dneregistry/report.pdf>.

ENFORCING PRIVACY PROMISES AND INFORMATION SECURITY

Another area of continuity is our effort to enhance security of information and ensure that privacy promises, once made, are kept. Protecting the security of information, once it is collected, remains the key to protecting consumer privacy. Our law enforcement, education, and rules all reinforce the common-sense principle: companies that process or store personal information about consumers have a responsibility to safeguard that data. Security is privacy in its most basic form. That is especially – but not only – true when the company has made specific promises about its security practices.

We have brought four cases to drive this message home.[12] In each case, the companies we sued did not have reasonable security procedures, despite promises to the contrary. Together, these cases spell out the four key points that guide our information security enforcement program. First, information security is an ongoing process of assessing risks and vulnerabilities. Security programs must adapt to evolving threats and new technology. Second, a company's security procedures must be reasonable and appropriate in light of the circumstances. Such circumstances include the company's size and complexity, the nature and scope of its activities, and the sensitivity of the consumer information it handles. Third, a breach does not necessarily show that a company failed to have reasonable security measures. Breaches happen even when companies take every reasonable precaution. Finally, a company's practices may be unreasonable even without a known security breach.

---

[12] *Eli Lilly & Co.*, Dkt. No. C-4047 (May 10, 2002); *Microsoft Corp.*, Dkt. No. C-4069 (Dec. 24, 2002); *Guess? Inc. and Guess.com., Inc*., Dkt No. C-4091 (Aug. 5, 2003); and *MTS, Inc., and Tower Direct, LLC*, Dkt. No. C-4110 (June 2, 2004). The complaints, decisions, and orders in these cases are available at <www.ftc.gov/privacy/privacyinitiatives/promises_enf.html>.

So what should an information security program involve? To answer this question, we look to the Gramm-Leach-Bliley Safeguards Rule.[13] This Rule requires financial institutions to ensure that they have security that is appropriate for the information they collect. Although the Safeguards Rule only applies to financial institutions, it serves as a useful guide for good information security practices in all industries. Indeed, the final orders in our four information security cases draw on the requirements of the Rule and, conversely, if the businesses followed the requirements of the Rule, they would not have faced the FTC law enforcement actions.

Now let's move from information security to information sharing. When companies promise to keep consumers' information private, consumers have every right to expect that promise will be kept. The FTC has brought several cases to stop companies from sharing consumers' personal information in violation of their own privacy policies.[14] That is a relatively straightforward principle. But what about changes to your privacy policy?

In *Gateway Learning*, a case announced in July, the company's privacy policy promised not to share consumers' information and said the company would notify consumers of any material changes to the policy.[15] We alleged that, despite these promises, Gateway rented consumers' information to marketers, changed its privacy policy but failed to notify consumers of the changes, and continued to rent information collected under the earlier policy.

---

[13]16 C.F.R. Part 314, available at http://www.ftc.gov/os/2002/05/67fr36585.pdf.

[14]*See, e.g., Educ. Research Center of America, Inc.*, Dkt. No. C- 4079 (May 6, 2003); *The Nat'l Research Center for College & University Admissions*, Dkt. Nos. C-4071 & C-4072 (Jan. 28, 2003).

[15]*In the matter of Gateway Learning Corp.*, File No. 042-3047 (July 7, 2004).

Our complaint alleged that Gateway's retroactive application of its new privacy policy to previously-collected information was unfair. Why was this practice unfair? Gateway unilaterally broke its promise to consumers and rented their information to marketers. Consumers were injured because their information was used for marketing purposes contrary to their expectations and without notice or the ability to prevent it. The *Gateway* consent agreement requires Gateway to obtain consent from consumers when it makes material changes to its privacy policy that will affect previously-collected information. The order also requires Gateway to give up the profits it made from renting the data.

Of course, companies may need to change their privacy policies from time to time. *Gateway* offers two lessons on this point. First, "do what you say." If companies promise to notify consumers of changes, they must do so. Second, don't change the rules after the game has been played. If companies collect information from consumers under one policy, they cannot retroactively apply a new, inconsistent policy to that data unless the consumer agrees.

IDENTITY THEFT AND FACTA

One of the most serious consequences of the misuse of information is identity theft. The FTC continues its fight against identity theft on several fronts. The implementation of The Fair and Accurate Credit Transactions Act of 2003 or "FACTA" is a key part of this program.[16] FACTA provides new and important measures to prevent identity theft and help identity theft victims to recover. We are investing enormous resources in FACTA; we have 45 people working on 20 rules and 8 studies. These rules and studies illustrate the importance of striking a

[16]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.*

balance between the benefits that an information society can provide to consumers, and the severe consequences that can result when consumer information is misused. Our goal here is to get this balance right!

Several FACTA provisions focus on prevention, but I will highlight just a few. First, beginning on December 1st, credit reporting agencies will be required to provide free credit reports to consumers.[17] This important new consumer benefit will be phased in over nine months in a "regional roll out" – beginning on the West Coast. Second, also beginning on December 1st, the credit reporting agencies will implement a National Fraud Alert System that will allow consumers to place a fraud alert on their credit files if they suspect or know that they have been victims of identity theft and require that creditors take certain steps to verify these consumers' identities before issuing credit.[18] Finally, businesses will have to truncate credit card and debit card account numbers on consumers' electronic receipts so that identity thieves who find or steal these receipts cannot take over these accounts.[19]

In addition to prevention, FACTA has provisions to help identity theft victims pull their financial lives back together. Here is just one example: FACTA will require credit reporting agencies and creditors to stop reporting allegedly fraudulent account information when a consumer establishes that she has been the victim of identity theft.[20] Overall, FACTA tries to be

---

[17]*See* 16 C.F.R. Part 610 (2004) (Free Annual File Disclosures Rule).

[18]Pub. L. No. 108-159, § 112 (2003).

[19]Pub. L. No. 108-159, § 113 (2003).

[20]Pub. L. No. 108-159, §§ 152, 154 (2003).

sure consumers are better educated about their credit rights, better armed to prevent identity theft, and better able to respond if their identities are stolen.

NEW CHALLENGES

New technology often raises issues involving consumers' expectations of privacy. This was the case with cameras, the telephone, the fax machine, the Web, chat rooms, and, of course, email. As with spam and information security, we have explored the privacy implications of new technologies. We have also sought to educate consumers about the potential privacy risks. And, when warranted, we have pursued law enforcement actions. As the nation's consumer protection agency, we will continue this approach as new technology raises new issues and new challenges. I'd like to discuss three technologies that have gained prominence since we launched our privacy agenda.

NEW CHALLENGES – RADIO FREQUENCY IDENTIFICATION

A great example of these new challenges is radio frequency identification or "RFID." RFID uses small tags that can be attached to consumer products. These tags store a unique identifier – or "electronic product code" – and can wirelessly transmit that code to a reader device.

As with other emerging information technologies, RFID has great potential benefits. Applications include inventory management, pharmaceutical drug safety, health care, and transportation. Consumers use RFID technology when they zip through "easy pass" lanes at toll booths. In addition to these benefits, however, there are also potential risks. Some fear that this technology will enable the tracking of individual products off the shelves, out of the store, and into consumers' homes. Privacy advocates are concerned about what information is being

collected, and how that information may be used, shared, and stored. Questions have also been raised about how to provide effective notice to consumers when RFID tags are being used.

Last June, the Commission convened a public workshop to explore the benefits and costs of RFID.[21] Since the workshop, we have continued to explore the evolution of RFID. For example, our staff is actively monitoring the development of industry best practices that may address consumers' privacy concerns. We have also participated in a number of domestic and international conferences. This winter, we plan to release a staff report summarizing the key issues raised at our workshop.

NEW CHALLENGES – PEER-TO-PEER FILE SHARING

Yet another "new" issue is the privacy implications of peer-to-peer file-sharing software. This software offers consumers the ability to share files – including music, video, or software – with other users. File sharing technology has numerous potential benefits for consumers. However, consumers also face potential risks when downloading and using P2P file-sharing programs. For example, consumers may unknowingly allow others to copy private files. They also may inadvertently download viruses or spyware or cause security breaches.

The FTC has initiated a two-part plan to address these concerns. First, we are educating consumers. We published an online consumer alert about file-sharing and, as of late September, over 100,000 consumers have viewed this brochure.[22] Similarly, P2P distributors are working to improve their risk disclosures. Second, we are educating ourselves on the benefits and risks of

---

[21]Transcripts from the workshop, *Radio Frequency Identification: Applications and Implications for Consumers*, are available at <www.ftc.gov/bcp/workshops/rfid/index.htm>.

[22]*File Sharing: A Fair Share? Maybe Not.* Available at <www.ftc.gov/bcp/conline/pubs/alerts/sharealrt.htm>.

P2P technology. On December 15 and 16, the Commission will host a public workshop on P2P file-sharing programs.[23] We intend to discuss current and future applications of the technology, risks to consumers, self-regulatory and technological efforts to protect consumers from these risks, and competition issues.

NEW CHALLENGES – SPYWARE

The third "new challenge," spyware, was the subject of an entire panel this morning. The prominence of this issue at today's conference is telling. After spam, spyware is becoming one of the most serious consumer problems on the Internet. Spyware can surreptitiously install itself on a computer and wreck havoc on your PC. It can flood you with pop-up ads, hijack your home page, track your Web surfing, and impair your PC's performance, even causing a crash. In some cases, it will monitor your key strokes and covertly harvest personal information like passwords or credit card numbers.

The FTC is combating this new digital threat with the same three-prong strategy that we have used to fight spam: enforcement, education, and research. On the law enforcement front, we just filed our first spyware case, *FTC v. Seismic Entertainment*.[24] In *Seismic*, we alleged that the defendants downloaded spyware to consumers' computers – without their knowledge or authorization. Defendants' spyware then inflicted a variety of harms on consumers. It modified their web browsers, hijacked their search engines, monitored their Internet activity, bombarded

---

[23]To encourage broad-based participation, the FTC issued a Federal Register Notice announcing the workshop and requesting public comment. The Federal Register Notice is available at <www.ftc.gov/os/2004/10/041015p2pfrn.pdf>. Additional information about the upcoming workshop, including a preview of the agenda, is available at <www.ftc.gov/bcp/workshops/filesharing/index.htm>.

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

them with pop-up ads and installed additional software, including spyware that could capture information they entered into online forms. As if this is not enough – after the defendants infected computers with their spyware, they aggressively advertised purported "anti-spyware" software. Defendants earned a handsome commission each time a consumer purchased this reputed anti-spyware software.

The FTC brought this case under our unfairness jurisdiction – not deception. Last week, the court entered a temporary restraining order against the defendants, halting the alleged unlawful activities. A preliminary injunction hearing is scheduled for January 4th. And, there are more cases on the way!

But we realize that, just as with spam, enforcement alone will not solve the spyware problem. When the FTC announced the *Seismic* case, we also released a new consumer alert to educate consumers about the problem of spyware.[25] We also held a workshop on spyware last April.[26] The workshop was designed to provide industry, policymakers, and consumers with information about the problems related to spyware. We hope to issue a report this winter on our findings.

GLOBAL ISSUES REQUIRE GLOBAL SOLUTIONS

Finally, I would point out, spyware, like spam and the other privacy issues I have discussed today, are global issues that require global solutions. For this reason, the FTC has undertaken a leadership role on international privacy and security issues. Chairman Majoras

---

[25]The consumer alert is available at <www.ftc.gov/bcp/conline/pubs/alerts/spywarealrt.htm>.

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

already has made international coordination and cooperation one of her top priorities. In fact, she just returned from the London Spam Enforcement Conference, the first international gathering on combating cross-border spam. The conference participants, including the FTC, endorsed the "London Action Plan on Spam," a concrete plan to help prosecute spammers wherever they may hide.

To improve our ability to fight cross-border fraud – including spam and spyware – we have recommended that Congress pass the International Consumer Protection Act.[27] This will give us necessary new tools to share and gather information and seek investigative assistance in cases where businesses defraud consumers across borders.

CONCLUSION

I could go on. The FTC is an exciting place to work, and we have a full agenda. However, I hope I said enough today to make my point: privacy protection efforts will continue to occupy a central role in our consumer protection mission. I look forward to your questions.

[27]As of October 28, 2004, the Senate has passed its version of the International Consumer Protection Act ("ICPA"), S. 1234. The House Judiciary Committee has reported out a version of ICPA, HR 3143, that is awaiting a vote by the full House.