Remarks of Howard Beales

Before the IAPP

June 2004*

The FTC and Consumer Privacy:

An Accomplished Agenda

*The published version of this speech contains Commission actions and activities through July 31, 2004. The views expressed are those of Mr. Beales and do not necessarily reflect the views of the Commission or of any individual Commissioner.

[1] Timothy J. Muris, *Protecting Consumers' Privacy: 2002 and Beyond, available* at <http://www.ftc.gov/speeches/muris/privisp1002.htm

for most consumers. Consider the billions of privacy notices sent to consumers under the Gramm-Leach-Bliley Act. Very few have exercised their right to opt-out of information sharing. Exercising just one opportunity to opt-out may take only a few minutes, but opting out for each of the companies a consumer does business with would take much longer. Consumers have many other things to do. Given that time is scarce and even reading the notice takes effort that could be spent elsewhere, it is not surprising that few consumers opt-out, even when it is seemingly easy. Opt-in doesn't work any better. Because most consumers will not expend the time and effort to consider the choice, opt-in is only the correct default if most fully-informed consumers would refuse to share information. But explaining the benefits and costs of information sharing is beyond the competence of even the best drafted short notices. In sum, the notice approach falls short because we cannot *make* people focus on this, or any other, issue.

There is no denying that surveys tell us that consumers *are* troubled by the extent to which their information is collected.[2] But, at the same tim

[2] That concern has been expressed in a number of public opinion polls. *See, e.g.,* Alan F. Westin/Harris Interactive, *Privacy On and Off the Internet: What Consumers Want* (Nov. 2001); IBM/Harris Interactive, *Multi-National Consumer Privacy Survey* (Oct. 1999); Lorrie Faith Cranor et al., *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy,* AT&T Labs-Research Technical Report TR 99.4.1 (Mar. 1999).

consequences drive consumer concerns about privacy. Our privacy agenda is focused on *stopping* the kinds of practices that can cause negative consequences for consumers.

For example, many consumers are concerned about *physical consequences.* Do you know any parents who want information on the whereabouts of their kids to be freely available to anyone? Of course not. The misuse of information can also cause *economic consequences,* including the improper denial of credit – or even a job – based on inaccurate or incomplete information. Misuse of information can also lead to identity theft. That has been our top consumer fraud complaint for three years in a row. Finally, the misuse of information can cause *annoying, irritating, and unwanted intrusions* in consumers' dail0000 0.0000ysT00000 l4Pon in

[3] This approach also reduces the transaction costs for consumers by making it easier to express their preferences about receiving telemarketing calls. *See* R.H. Coase, *The Problem of Social Cost,* 3 J. L. & ECON. at 15-16.

[4] One example of the exception's benefits is for consumers who subscribe to a magazine and also register for the National Do Not Call Registry. When the subscription is about to end, the telemarketer for the magazine can call the consumer and ask if she wants to renew without violating the Do Not Call provision of the Telemarketing Sales Rule. For the many consumers who desire to renew but ignore mail requests, this phone call is beneficial.

Nonetheless, like any rule, this one needs enforcement. This spring, the Commission filed its first Do Not Call case against National Consumer Council.[6] This case is typical of the top violators subject to our jurisdiction, in that there is a combination of a Do Not Call problem and other problems. The Commission's complaint alleges that NCC misrepresented itself as a non-profit debt negotiation organization that, for an up-front fee, would reduce consumers' debts. In fact, we allege, the company took consumers' money but did not negotiate on their behalf, and did not have any arrangements in place to achieve any such debt reduction. Moreover, we allege, NCC was not in fact a non-profit organization. Finally, in addition to these misrepresentations to consumers, we allege that NCC called consumers who had placed their numbers on the National Do Not Call Registry.

Spam

Like unsolicited telemarketing, unsolicited commercial email – or spam – has become a major source of annoyance and deception. Left unchecked, many predict that spam will overwhelm our email system. Indeed, spam is one of the most daunting consumer protection problems that the Commission has ever faced. The problems go well beyond the annoyance it causes. They include the fraudulent and deceptive content of a large percentage of spam messages, the offensive content of many spam messages, the sheer volume of spam being sent across the Interne

[6] *FTC v. Nat'l Consumer Council*, No. SACV 04-0474 CJC (JWJx) (C.D. Cal. filed Apr. 23, 2004).

The National Do Not Call Registry protects consumers from the unwanted intrusion of telemarketing calls while not unduly inhibiting the flow of useful information. No similar solution exists for spam. At Congress's request, the Commission conducted a thorough study of the possibility of a do not email list. We found that such a system would not work, and could well make the problem worse. Why? Well, first, because spam is virtually untraceable, a do not email list would be extremely difficult to enforce. More importantly, any do not email system must tell marketers, directly or indirectly, who is on the list. That gives spammers the one thing that is otherwise difficult for them to obtain – a list of valid email addresses. For spam, anonymity is a better solution than a registry. People who signed up for a registry could well find that the amount of spam they receive increases.[7]

The Commission has pursued a three-fold strategy to combat the plague of spam. First, it has pursued a vigorous program of law enforcement against spammers, both before the enactment of CAN-SPAM and since it became effective on January 1, 2004. Second, we have an extensive education program to alert consumers and businesses about self-help measures they can take against spam. Third, we have studied the problem of spam to inform our enforcement and consumer education efforts, and to remedy the paucity of reliable data about spam.

---

[7] 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.>. In preparing this report, the Commission staff conducted interviews with more than 80 individuals representing 56 different organizations. It solicited public comment, issued a request for information from potential contractors, and hired three independent technical experts to help evaluate the feasibility of a registry.

Law Enforcement

The Commission has brought 62 law enforcement actions in recent years against alleged fraudulent operations using spam as an integral component of their scams. Most of these cases predate CAN-SPAM, and were brought under Section 5 of the FTC Act.[8] Two of our most recent spam cases, filed in federal district court in April, target extremely prolific spammers and allege violations of both CAN-SPAM and the FTC Act.[9]

The Commission's complaint in the first of these cases,

---

[8] 15 U.S.C. § 45.

[9] *See* <http://www.ftc.gov/opa/2004/04/040429canspam.htm>.

[10] Case No. 04C 2897 (N.D. Ill. filed Apr. 23, 2004).

[11] In investigating and filing this matter, the Commission worked closely with the U.S. Attorney for the Eastern District of Michigan and the Detroit Office of the Postal Inspection Service, who are pursuing a concurrent criminal prosecution of the principals of this scheme.

agencies, which has targeted deceptive spam. This partnership includes the Department of Justice, FBI, Postal Inspection Service, Securities and Exchange Commission, and Commodities Futures Trading Commission, as well as state Attorneys General, and local enforcement officials. In four regional law enforcement sweeps, the most recent announced in May 2003, the Netforce partners filed more than 150 criminal and civil cases against allegedly deceptive spam and other Internet fraud.[13] In one recent sweep case, for example, the Commission obtained a permanent spam ban against defendants who allegedly used deceptive "from" lines in their spam to claim affiliation with Hotmail and MSN in touting a fraudulent work-at-home envelope-stuffing scheme.[14]

The Commission remains committed to aggressive pursuit of spammers who violate Section 5 of the FTC Act and the CAN-SPAM Act, and we remain committed to working with our law enforcement partners to find and take action against spammers. Law enforcement is essential, but enforcement alone cannot abate the flood of spam.

Consumer and Business Education about Spam

The Commission's educational efforts include a spam home page with links to publications for consumers and businesses, including one in Spanish, and summaries of our

---

[13] More information about the Netforce law enforcement sweeps is available on the FTC's web site: <http://www.ftc.gov/opa/2002/04/spam.htm> (Northwest Netforce); <http://www.ftc.gov/opa/2002/07/mwnetforce.htm> (Midwest Netforce); <http://www.ftc.gov/opa/2002/11/netforce.htm> (Northeast Netforce); and <http://www.ftc.gov/opa/2003/05/swnetforce.htm> (Southwest Netforce).

[14] *FTC v. Patrick Cella, et al.*, No. CV-03-3202, (C.D. Cal. Nov. 21, 2003) (final order). *See* <http://www.ftc.gov/opa/2003/05/swnetforce.htm>; <http://www.ftc.gov/opa/2003/11/dojsweep.htm>.

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

[16] Most organizations have multiple computers on their networks, but have a smaller number of "proxy" servers – the only machines on the network that directly interact with the Internet. This system provides more efficient Web browsing for the users within that organization and secures the organization's network against unauthorized Internet users from outside the organization. If the proxy is not configured properly, it is considered to be "open," and may allow an unauthorized Internet user to connect through it to other hosts (computers that control communications in a network or administer databases) on the Internet. In this way, open proxies provide one of several methods that spammers use to hide their identities.

[17] The press release can be found at <http://www.ftc.gov/opa/2004/01/opsecure.htm>. Tens of thousands of owners or operators of potentially open relay or open proxy servers around the world received the Operation Secure Your Server business education letter.

[18] An open relay is an email server that is configured to accept and transfer email on behalf of any user anywhere, including unrelated third parties, which allows spammers to route their email through servers of other organizations, disguising the origin of the email. By contrast, a "secure" server accepts and transfers mail only on behalf of authorized users. *See* FTC Facts for Business, *Open Relays – Close the Door on Spam* (May 2003), *available at* <http://www.ftc.gov/bcp/conline/pubs/buspubs/openrelay.htm>.

[19] On January 28, 2004, the FTC issued a consumer alert – "Who's Spamming Who? Could It Be You?" – warning consumers that their home computers could also be commandeered by spammers to send spam without their knowledge or consent. This consumer alert explained how consumers could avoid this misuse of their computers, how to determine if

Studies and Workshops

Everybody receives spam, but reliable information about it is extremely limited. Nonetheless, there is much "spam lore" that has little if any basis in fact. For example, some sources in Europe claim that the vast majority of spam originates in the United States.[20] Similarly, some sources in the U.S. opine that most spam in Americans' in-boxes arrives from Asia, South America, or Eastern Europe.[21] In fact, nearly all spam is virtually untraceable, either because it contains falsified routing information or because it comes through open proxies or open relays.[22] Moreover, "spoofing" and "forging"[23] of an email message's "from" line and

---

their computers were being exploited, and how to stop the misuse if it was occurring. This consumer alert can be found at <http://www.ftc.gov/bcp/conline/pubs/alerts/whospamalrt.htm>.

[20] *See* <http://www.informationweek.com/story/showArticle.jhtml?articleID=18200812; http://www.spamhaus.org/news.lasso?article=150>.

[21] In fact, some sources estimate that anywhere from 30-80% of spam is routed through open relays and open proxies, and many of these machines are scattered throughout the world. *See* <http://news.zdnet.co.uk/hardware/emergingtech/0,39020357,2122679,00.htm>; <http://www.cnn.com/2004/TECH/ptech/02/17/spam.zombies.ap/>.

[22] In Congressional testimony last year, Brightmail estimated that 90% of the email that it analyzed was untraceable. <http://www.brightmail.com/pressreleases/102203_senate_bill_877.html>. At the FTC's May 2003 Spam Forum two panelists representing ISPs estimated that 40% to 50% of the email they analyzed coming to or through their networks made use of open relays or open proxies, making it virtually impossible to trace. FTC Spam Forum transcript, Day 1, *Open Relay, Open Proxies, and Formmail Scripts Panel*, pp. 257, 274, *available at* <http://www.ftc.gov/bcp/workshops/spam/>.

[23] "Spoofing" and "forging" involve manipulating an email's "from" line or header information to make it appear as if the message were coming from an email address from which it did not actually originate.

[24] At the FTC Spam Forum, Margot Koschier from AOL conducted a live demonstration of how to forge header information. In several minutes, she was able to send a message that appeared to come from FTC Chairman Tim Muris in the year 2024. Other Spam Forum panelists also discussed the prevalence of false "sender" information in spam. For example, an MCI representative stated that 60% of the spam complaints received at MCI have false headers, false email addresses, deceptive subject lines, or a combination of all three. *See* FTC Spam Forum transcript, Day 1, *Falsity in Spam Panel*, *available at* <http://www.ftc.gov/bcp/workshops/spam/>.

[25] This uncertainty is reflected, for example, in six lawsuits jointly announced by several ISPs on March 10, 2004. They sued nine individuals, and over 200 unknown "John Does." *See* Joint press release of AOL, Earthlink, Microsoft, and Yahoo!, *available at* <http://www.microsoft.com/presspass/press/2004/mar04/03-10CANSPAMpr.asp>. Similarly, in

fact, the low barriers to entry suggest that many individuals, and not just a handful, may engage in spamming and contribute significantly to the volume of spam traversing the Internet.[26]

The prevalence of "spam lore" of questionable validity and the corresponding paucity of reliable data on spam has prompted the FTC's staff to conduct research on the issue. In one of the first of these efforts, the Commission's staff, working with a partnership of law enforcement officials in several states and Canada,[27] conducted a "Remove Me" surf in 2002 to test whether spammers were honoring "remove me"or "unsubscribe" options in spam. From email that the partnership had forwarded to the FTC's spam database, the Commission's staff selected more than 200 messages that purported to allow recipients to remove their names from a spam list. To test these "remove me" options, the partnership set up unique email accounts that had never been used before and submitted "remove me" requests from these accounts. The staff found that 63 percent of the removal links and addresses in the sample did not function. If a return address does not work to receive return messages, it is unlikely that it could be used to collect valid email addresses for use in future spamming. In no instance did we find that any of our unique email accounts received more spam after attempting to unsubscribe. This finding is inconsistent with

---

[26] *See* remarks of Laura Betterly at the FTC Spam Forum. Betterly stated that she paid $15,000 for her email business and broke even within 3 months. FTC Spam Forum transcript, Day 2, *Economics of Spam Panel*, pp. 28-29, *available at* <http://www.ftc.gov/bcp/workshops/spam/transcript_day2.pdf>.

[27] The "Remove Me" surf was conducted as part of the Northwest Netforce, an enforcement sweep in which the FTC was joined by the Alaska Attorney General, the Alaska State Troopers, Government Services of the Province of Alberta, the British Columbia Securities Commission, the British Columbia Solicitor General, the Canadian Competition Bureau, the Idaho Attorney General, the Montana Department of Administration, the Oregon Department of Justice, the Washington Attorney General, the Washington State Department of Financial Institutions, and the Wyoming Attorney General. *See* <http://www.ftc.gov/opa/2002/04/spam.htm>.

the common belief that attempting to unsubscribe guarantees that consumers will receive more spam.[28]

Another study in 2002, the "Spam Harvest," examined what online activities place consumers at risk for receiving spam.[29] We discovered that all of the email addresses that we posted in chat rooms received spam. In fact, one address received spam only *eight minutes* after the address was posted. Eighty-six percent of the email addresses posted in newsgroups and web pages received spam, as did 50 percent of addresses in free personal web page services, 27 percent in message board postings, and 9 percent in email service directories. The "Spam Harvest" also found that the type of spam received was not related to the sites where the email addresses were posted. For example, email addresses posted in children's newsgroups received a large amount of adult-content and work-at-home spam.[30]

A third study focused on false claims in spam by analyzing a sample of 1,000 messages drawn from three sources.[31] The Commission staff issued a report on April 30, 2003, explaining

---

[28] *See* <http://www.ftc.gov/bcp/conline/edcams/spam/pubs/removeme.pdf>.

[29] The "Spam Harvest" was conducted as part of the Northeast Netforce, an enforcement sweep in which the FTC was joined by the Connecticut Attorney General, the Maine Attorney General, the Massachusetts Attorney General, the New Hampshire Department of Justice, the New Jersey Division of Consumer Affairs, the New York City Department of Consumer Affairs, the New York State Attorney General, the New York State Consumer Protection Board, the Rhode Island Attorney General, the United States Attorney for the District of Massachusetts, the United States Postal Inspection Service, and the Vermont Attorney General. *See* <http://www.ftc.gov/opa/2002/11/netforce.htm>.

[30] *See* http://www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.htm>.

[31] The study's sources were the FTC's database of millions of spam forwarded to the Commission by consumers, messages received in the "Spam Harvest," and messages delivered to FTC employees' email accounts.

[32] *False Claims in Spam*: *A Report by the FTC's Division of Marketing Practices* (April 30, 2003), *available at* <http://www.ftc.gov/reports/spam/030429spamreport.pdf>. Sample spam analyzed in the study came from multiple sources, including the FTC's own spam database. In a random sample of 1,000 pieces of spam, 84.5 percent were deceptive on their face and contained apparently false "from" lines, "subject" lines, or message text, or advertised an illegitimate product or service.

[33] None of the spam in this sample was sent by a

the Forum brought forward an enormous amount of information about spam and how it affects consumers and businesses. Several primary themes emerged from the various panels. First, there was much discussion about the increasing amount of spam. Second, spam imposes real costs. The panelists offered concrete information about the costs of spam to businesses and to ISPs. Specifically, ISPs reported that costs to address spam increased dramatically in the two years immediately preceding the Forum. ISPs bear the cost of maintaining servers and bandwidth necessary to channel the flood of spam, even that part of the flood that is filtered out before reaching recipients' in-boxes. At the Forum, America Online reported that it blocked an astonishing 2.37 billion pieces of spam in a single day.

---

[35] FTC Spam Forum transcript, Day 1, *Introduction to Spam Panel*, p. 39, *available at* <http://www.ftc.gov/bcp/workshops/spam/transcript_day1.pdf>.

[36] 15 U.S.C. § 7701 *et seq.*

Moreover, to facilitate enforcement by other law enforcement agencies, we have consulted with our partners at the Department of Justice and have organized a task force with state officials to bring cases. The Task Force is co-sponsored by the FTC and the Attorney General of Washington, and is comprised of 136 members representing 36 states, several units within the Department of Justice, and the FTC.[37] The FTC staff so far has conducted two training sessions on investigative techniques for the Task Force, each of which was attended by approximately 100 individuals representing about 35 different states. The Task Force conducts monthly conference calls to share information on spam trends, technologies, investigative techniques, targets, and cases.

The Commission is also on target to complete the rulemakings and reports required by CAN-SPAM. On January 28, 2004, the Commission issued a Notice of Proposed Rulemaking for a mark or notice that will identify spam containing sexually oriented material.[38] The Commission received 89 comments in response.[39] We issued a final rule in advance of the statutory deadline of April 14.[40] Effective May 19, the rule requires all messages containing sexually oriented material to include the warning "SEXUALLY-EXPLICIT" in the subject line. This rule also prohibits these messages from presenting any sexually explicit material in the

---

[37] The Commission continues to try to recruit representatives from the remaining states.

[38] 69 Fed. Reg. 4263 (Jan. 29, 2004).

[39] *Available at* <http://www.ftc.gov/os/comments/adultemaillabeling/index.html>.

[40] *See* <http://www.ftc.gov/opa/2004/04/adultlabel.htm>.

begin widespread testing and deployment of authentication standards. Hopefully, such efforts can help both government and the private sector staunch the flow of spam.

Identity Theft

Our privacy agenda is built around concern for the consequences of misuse of information. One of the most serious consequences of misuse is identity theft. The FTC addresses this problem with three main components: our Identity Theft Data Clearinghouse (the "Clearinghouse"); our consumer education and assistance resources, including our toll-free hotline, web site, and educational brochures; and our collaborative and outreach efforts with law enforcement and private industry.

The FTC's primary role in combating identity theft derives from the 1998 Identity Theft Assumption and Deterrence Act ("the Identity Theft Act" or "the Act"),[51] which directed the Commission to establish a central repository for identity theft complaints and to provide victim assistance and consumer education. The Clearinghouse now contains over 600,000 identity theft complaints taken from victims across the country. By itself, though, these self-reported data do not currently allow the FTC to draw any firm conclusions about the incidence of identity theft in the general population.

Identity Theft Survey

To address this important issue, the FTC commissioned a survey last year to gain a better understanding of the incidence of identity theft and the impact of the crime on its victims.[52] The

---

[51] 18 U.S.C. § 1028.

[52] The research took place during March and April 2003. It was conducted by Synovate, a private research firm, and involved a random sample telephone survey of over 4,000 U.S. adults. The full report of the survey can be found at

[53] Pub. L. No. 108-396 (2003) (codified at 15 U.S.C. § 1681 *et seq.*).

[54] 15 U.S.C. § 1681 *et seq.*

[55]

credit reports to consumers once annually, upon request.[59] Free reports will enhance consumers' ability to discover and correct errors, thereby improving the accuracy of the system, and also enable consumers to detect identity theft early.

Other measures that act to prevent identity theft include:

- *National fraud alert system*.[60] Consumers who reasonably suspect they have been or may be victimized by identity theft, or who are military personnel on active duty away from home,[61] can place an alert on their credit files. The alert will put potential creditors on notice that they must proceed with caution when granting credit in the consumer's name. The provision also codified and standardized the "joint fraud alert" initiative administered by the

---

[59] *See* Free Annual File Disclosures, 16 C.F.R. §§ 610.1 and 698.1 (2004).

[60] Pub. L. No. 108-396, § 112 (2003).

[61] The Commission is developing a rule on the duration of this active duty alert. *See* Related Identity Theft Definitions, Duration of Active Duty Alerts, and Appropriate Proof of Identity Under the Fair Credit Reporting Act, 69 Fed. Reg. 23370, 23372 (April 28, 2004) (to be codified at 16 C.F.R. pt. 613).

[62] Pub. L. No. 108-396, § 113 (2003).

[63] FACTA creates a phase-in period to allow for the replacement of existing

• *Identity theft account blocking.*[68] This provision requires credit reporting agencies immediately to cease reporting, or block, allegedly fraudulent account information on consumer reports when the consumer submits an identity theft re 0.00.1200 Tc-0.12n144.0000 708.72000.0a.00

[68] Pub. L. No. 108-396, § 152 (2003).

[69] The Commission is developing a rule to define the term "identity theft report." *See* Related Identity Theft Definitions, Duration of Active Duty Alerts, and Appropriate Proof of Identity Under the Fair Credit Reporting Act, 69 Fed. Reg. 23,370, 23,371 (Apr. 28, 2004) (to be codified at 16 C.F.R. pt. 603).

[70] Pub. L. No. 108-396, § 151 (2003).

[71] *Id*. § 154.

(y)Tj5.2.7200 0.0000 TDoeport debe

When fully implemented, these provisions should help to reduce the incidence of identity theft, and help victims recover when the problem does occur.

Furthermore, the FTC has committed significant resources to assisting criminal law enforcement prosecute ID thieves. Investigation and prosecution not only stop the offender from destroying another person's financial well being, but also can deter would-be identity thieves from committing the crime. Congress recently enacted legislation to increase penalties for those convicted of identity theft.[72]

One area where the FTC has used its own civil law enforcement resources to combat identity theft is in the fight against "phishing." In this scam, identity thieves send spam that appears to originate from some institution with which the consumer has an account, such as an ISP or a financial institution. The spam claims that the consumer needs to update their billing information, and offers a convenient link to a look-alike web site that is designed to mimic the legitimate pages of the company. The scammers ask for credit card numbers, passwords, Social Security numbers, and other information, which they use to make purchases on the consumer's account or to open new accounts in the victim's name. Working closely with the criminal authorities, the Commission has obtained civil injunctions in three "phishing" cases to date.[73]

---

[72] The Identity Theft and Enhancement Penalty Act, P.L. 108-275, was signed into law on July 15, 2004.

[73] *FTC v. C.J.*, CIV-03 5275 GHK (RZx) (C.D. Cal. July 24, 2003) (final order); *FTC v. Hill*, CV-H-03-5537 (S.D. Tex. Dec. 3, 2003) (final order); and *FTC v. M.M.*, CV-04-2086 (E.D. N.Y. May 18, 2004) (final order) (defendants sent "phishing" spam purporting to come from AOL or Paypal and created look-alike web sites to obtain credit card numbers and other financial data from consumers that defendants used for unauthorized online purchases).

Enforcing Privacy Promises

When companies promise to keep consumers' information private, consumers have every right to expect that promise will be kept. We have undertaken aggressive enforcement against companies who violate privacy promises, with a particular focus on promises made about the security provided for consumer information. Here again, we focus on misuses of information that causes adverse consequences – in this case, the use of information for purposes different from those consumers bargained for or in a manner that creates unreasonable risks that information will be misused. Our focus on adverse consequences also makes us particularly concerned about misuses of sensitive information – for example, credit card and Social Security numbers, medical data, and information about children.

Ensuring information security is a particular priority at the Commission. Poor security practices put consumer information at risk and can ultimately lead to identity theft or other serious misuses of information. We have brought four cases challenging promises companies made about the security provided for consumer information – against *Eli Lilly*,[74] *Microsoft*,[75] *Guess*,[76] and *Tower Records*.[77] Each case involved the failure to implement reasonable security procedures to protect sensitive information, despite promises to the contrary. The Eli Lilly case involved inadvertent disclosure of sensitive information about consumers' health. Although the breach was inadvertent, we asked whether the company had in place reasonable procedures,

---

[74] *Eli Lilly & Co.*, Dkt. No. C-4047 (May 10, 2002).

[75] *Microsoft Corp.*, Dkt. No. C-4069 (Dec. 24, 2002).

[76] *Guess? Inc. and Guess.com., Inc.*, Dkt No. C-4091 (Aug. 5, 2003).

[77] *MTS, Inc., and Tower Direct, LLC*, Dkt. No. C-4110 (June 2, 2004).

appropriate in light of the sensitivity of the information, to prevent such breaches. We thought they did not.

Our case against Microsoft establishes the principle that there can be a law violation even in the absence of a proven breach of security. The Commission's complaint alleged that Microsoft's Passport authentication system and Passport Wallet, which included credit card information, did not include sufficient safeguards to protect the information, given its sensitivity. In particular, the complaint alleged that Microsoft lacked adequate systems to prevent unauthorized access, to detect such access if it occurred, to monitor the system for vulnerabilities, and to record sufficient information to enable investigations after the fact.

The *Guess* case highlights the importance of maintaining an ongoing program to adapt information systems to new security threats. The complaint in the *Guess case* alleged that the company's web sites was vulnerable to a well known "web based application" vulnerability. In essence, the complaint alleged that *Guess* had no procedures to monitor for known application vulnerabilities, or to detect and block attacks when they occurred. Even if the system was state of the art when it was first installed, companies have an obligation to monitor that system, and make reasonable changes to address new threats.

The Commission's settlement with *Tower Records* also highlighted the need to make sure that companies do not introduce new problems in the course of fixing old problems or making improvements to a company's system. In introducing system upgrades, Tower left out the codes to authenticate the user. That meant that any user could get access to consumers' purchase history.

78

Sharing information with third parties was also the subject of our latest privacy case against *Gateway Learning Corp.*[80] Our complaint alleges that Gateway rented the information to marketers, contrary to explicit promises in its privacy policy that it would not do so. The marketers used this information – which included name, address, phone number, and the age range and gender of the customers' children – to send mailings and make telemarketing calls to Gateway's customers.

Gateway was also the first case to challenge a company's practices in making material changes to its privacy policy. We alleged that, after collecting the information, Gateway changed its privacy policy to allow it to share the information but did not notify customers who had already given their information or obtain their consent to the change. Gateway therefore made a material change to its privacy policy which it applied to information it had already collected – a practice we regard as unfair. Gateway changed its policies without following the process it agreed to in its privacy policy – namely, to notify consumers of material changes to the policy so consumers had an opportunity to opt out of those changes. To remedy these violations, the proposed consent agreement bars future misrepresentations and also requires Gateway to get consent from consumers before making material changes to its privacy policy that affect information already collected. These are important remedies to ensure that the company keeps its promises in the future. The order also requires Gateway to give up the profits it made from renting the data – the first privacy case to involve financial remedies.

We understand that companies need to change their privacy policies from time to time. And this case stands for two important propositions regarding such changes. First, if a privacy

---

[80] *Gateway Learning Corp.*, File No. 042-3047 (July 7, 2004).

policy sets out a process for making changes, companies must follow that process. If they promise notice, they must give notice. Quietly posting a new policy on a web site will not do. Second, if companies collect information from consumers under one policy, they cannot retroactively apply a new, inconsistent policy to that data unless the consumer agrees. Changing the rules after the game has been played is unfair. A company that promises information will never be used for marketing cannot revoke that promise unless consumers agree.

Consumer Information Security

Information security is a core part of any program of preventing misuse of information. Good security is important to prevent theft and other misuses of sensitive information. If there was any doubt, consider the TriWest[81] and Ford/Experian[82] incidents, in which major breaches of company databases put the sensitive personal information of tens of thousands of consumers at risk. To prevent these harms, we are emphasizing security on a number of fronts.

First, as just discussed, we have challenged false statements companies make about their security practices. These cases appear to be having an effect. We understand that word is spreading, that companies are changing their practices, and that our cases are helping employees convince their CEOs to take appropriate care in this area.

We also have an important new tool, the Gramm-Leach-Bliley Safeguards Rule, to help us promote and enforce good security practices. Under the Rule, financial institutions must take certain basic steps to ensure that they have security appropriate for their businesses and for the

---

[81] Adam Clymer, *Officials Say Troops Risk Identity Theft After Burglary*, N.Y. TIMES, Jan. 12, 2003, § 1 (Late Edition), at 12.

[82] Kathy M. Kristof & John J. Goldman, *3 Charged in Identity Theft Case*, LA TIMES, Nov. 6, 2002, Main News, Part 1 (Home Edition), at 1.

The Future

You can expect a lot more from the FTC on the privacy front. Our top priority is spam, where we are devoting substantial resources to the pursuit of cases and we will continue that effort. We are working closely with the criminal authorities as they prepare to invoke the criminal liability features of CAN-SPAM when spammers fail to reveal their true identity.

Also high on our agenda is the FACT Act. We have numerous rule-making studies that are ongoing, that are eating a significant share of our resources. At the same time, we are engaged in enforcement activities under the Fair Credit Reporting Act, including a recent case where we obtained the largest civil penalty in a FCRA case.[85] Other cases enforcing the notice requirements of the FCRA will be forthcoming shortly.

Information security remains a high priority. Without information security there is no privacy and whatever notice or choice consumers may have thought they exercised is meaningless. We will continue to pursue cases in this important area.

And, finally, we will continue to bring Do Not Call enforcement actions. More cases are

[85] *United States v. NCO Group, Inc.* (E.D. Pa. Filed May 12, 2004) *available at*: <http://www.ftc.gov/opa/2004/03/ncogroup.htm>.