GREENBERG TRAURIG, LLP
200 Park Avenue
P.O. Box 677
Florham Park, New Jersey 07932-0677
(973) 360-7900 (Phone)
(973) 301-8410 (Facsimile)
Philip R. Sellinger (PS-9369)
Ian S. Marx (IM-1704)
Attorneys for Plaintiff, Cellco Partnership d/b/a Verizon Wireless

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

CELLCO PARTNERSHIP d/b/a VERIZON WIRELESS,	**Civil Action**
Plaintiffs,	**VERIFIED COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF, JURY DEMAND and CERTIFICATIONS (LOCAL RULES 11.2 AND 201.1(d)(3))**
vs.	
JOHN and JANE DOES I to XX,	
Defendants.	

Plaintiff CELLCO PARTNERSHIP d/b/a VERIZON WIRELESS (hereinafter "Plaintiff," "Verizon Wireless," or "the Company"), by and through its undersigned counsel, sues the Defendants, JOHN and JANE DOES I to XX (collectively "Defendants"), and alleges:

NATURE OF THE ACTION

1. Verizon Wireless brings this action to protect its customers' confidential information from Defendants, who have attempted to obtain that information through unlawful "pretexting" schemes.

PARTIES, JURISDICTION, AND VENUE

2. Verizon Wireless is a Delaware general partnership with its principal place of

business at One Verizon Way, Basking Ridge, New Jersey 07920.

3. Defendants John and Jane Does I through XX, whose identities and addresses are presently unknown to Verizon Wireless, are individuals or entities who: (a) were retained, directly or indirectly, by the Hewlett-Packard Company ("HP") in 2005 and 2006 to investigate any leaks of confidential information from HP's Board of Directors and have attempted to obtain confidential information on Verizon Wireless customers by making "pretexting" calls to Verizon Wireless customer care centers or by illicitly accessing Verizon Wireless' protected computers and data storage facilities; and/or (b) received proceeds from the sale of confidential Verizon Wireless customer information.

4. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331 and 18 U.S.C. § 1030(g) because the action arises under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. Pursuant to 28 U.S.C. § 1367, this Court has supplemental jurisdiction over the state law claims.

5. Venue is proper in this Court under 28 U.S.C. § 1391 because Defendants have caused tortious injury within the District of New Jersey, and because a substantial part of the events giving rise to the claim occurred in New Jersey, or were directed toward Verizon Wireless in this district.

FACTUAL ALLEGATIONS COMMON TO ALL COUNTS

Verizon Wireless' Safeguards

6. Verizon Wireless goes to great lengths to protect confidential customer information. Its customer service representatives ("CSRs") receive extensive training and communications on customer privacy issues, including the threat presented by illegal data brokers and the identification of the schemes they employ to obtain confidential customer information. No confidential customer information may be disclosed unless and until the CSR

has fully verified the customer.

7. Verizon Wireless is also committed to protecting the integrity of its systems that provide online access to account information. Customers can manage their accounts and access certain account information online, including call detail records, but cannot access other personally identifiable information, such as social security numbers, or usable credit card or bank account information. A user cannot establish or access an account online unless and until he or she has been fully verified by the online system.

8. Despite the precautions taken by Verizon Wireless to preserve the confidentiality of its customers' information, Defendants used fraud, trickery and deceit to access confidential customer information by making "pretexting" phone calls to Verizon Wireless customer service centers and obtaining unauthorized online account access.

The HP Investigation

9. On September 6, 2006, HP filed a Form 8-K with the United States Securities and Exchange Commission. (HP's 8-K is annexed hereto as Ex. 1.) The 8-K reported that, since at least 2005, HP was the subject of multiple leaks of confidential information, including information concerning the internal deliberations of its Board of Directors. HP further stated in the 8-K that, in response to those leaks, it retained, directly and indirectly, contractors and subcontractors to investigate the source of the leaks. The identities of those contractors and subcontractors who obtained confidential information of Verizon Wireless customers (collectively, Defendants John Does I through XX and Jane Does I through XX) are unknown. Plaintiff will amend this complaint once it learns their identities.

10. HP stated in the 8-K that a John Doe Defendant employed "pretexting" in an attempt to collect confidential telephone records information of HP Directors. "Pretexting" is a

method used by data brokers or other "investigators" to gain access to confidential information through deceit, often by impersonating a Verizon Wireless customer or employee. In general, data brokers collect private information about subscribers from various sources, and then fraudulently and deceptively use that information to trick customer service representatives into providing other private information, such as call detail records. The most common ruse involves posing as the customer or as an employee of Verizon Wireless, In addition, data brokers may use customer information to access a Verizon Wireless computer system (such as the system that provides online access to account information) to obtain private information on an account.

11. HP further acknowledged in subsequent statements that its investigators attempted to obtain telephone call records not only of HP Directors, but also of nine journalists and others. (See *HP Spied on Writers in Leaks*, The New York Times, September 8, 2006, annexed hereto as Ex. 2; *Hewlett Review Is Said to Detail Deeper Spying*, The New York Times, September 18, 2006, annexed hereto as Ex. 3.) Press accounts indicate the HP investigation began in or around January 2005. (See *Hewlett Review*, Ex. 3.) The California Attorney General and U.S. Department of Justice have each indicated that they are conducting investigations of the pretexting activity. (See *House Panel and U.S. Attorney Join H.P. Inquiry*, The New York Times, September 12, 2006, annexed hereto as Ex. 4.) On information and belief, additional private detectives were hired on behalf of HP to obtain phone records of HP Directors. (See *Panel Adds 5 Investigators to HP Data Hearing*, Reuters, September 27, 2006, annexed hereto as Ex. 5.)

Facts Regarding Verizon Wireless Accounts

12. Following HP's public disclosures, Verizon Wireless determined that account records of an HP Director (the "HP Director") were subject to unauthorized access by one or

more Defendants in May 2005, January 2006, and February 2006. Moreover, Defendants attempted to gain, and may have successfully gained, unauthorized access to the account of the HP Director's spouse.

(a) The HP Director's Account

13. On or about May 17, 2005, a Verizon Wireless CSR received a call from a person posing as a fellow Verizon Wireless employee ("Jane Doe I"). During the call, Jane Doe I indicated she was attempting to obtain access to the HP Director's account but was unable to do so. On information and belief, Jane Doe I attempted to gain confidential information about the account during this call.

14. On May 20, 2005, another call was made to Verizon Wireless customer service relating to this account. This call resulted in the blocking of text messages to the HP Director's wireless phone.

15. Minutes later, on May 20, 2005, records demonstrate that someone obtained online access to the account by meeting the necessary verification procedures. The user then changed both the user id and the e-mail address associated with the account. Verizon Wireless cannot determine what account information was accessed during this online session. On information and belief, the May 20 phone call, which resulted in the blocking of text messages, was an effort to prevent any text message alert from being sent to the customer's wireless phone. The calls to customer service on May 17 and May 20, and the online access to the account shortly thereafter, all provide evidence that Defendants gained unauthorized access to the account.

16. Although the HP Director terminated Verizon Wireless service on November 1, 2005, the account remained active with a secondary line. A second instance of unauthorized

access occurred on or about February 1, 2006. On that date, a call was made to a CSR indicating that the second line user lost her phone, could not remember her phone number because it had been changed, and wanted to call the phone before suspending service. In fact, the phone number had never been changed since the line was established. Accordingly, the purpose of this call was apparently to obtain the phone number of the secondary line.

17. Records further indicate that, also on or about February 1, 2006, someone obtained online access to the HP Director's account by meeting the necessary verification procedures and changing the password on the account. A different IP address was used to access the account on February 1 than had been used to access the account in the past. This same IP address was later used to access the online account on February 17. Verizon Wireless cannot determine what account information was accessed during these online sessions.

18. The foregoing acts demonstrate that Defendants used pretexting to gain unlawful access to the HP Director's account in February 2006.

(b) The Account of the HP Director's Spouse

19. At least three attempts were made to gain unauthorized access through customer service to the account of the HP Director's spouse. These attempts appear to have been unsuccessful, but online access may have been obtained.

20. Verizon Wireless records show that, on February 2, 2006, a person posing as a Verizon Wireless representative called a CSR seeking information on the account. The CSR added a "hot remark" on the account stating that the other CSRs should not give out any information without verifying the caller's information.

21. Minutes later, this account was registered online by establishing a user name and password. The IP address used to establish this account is the same IP address that was used to

access the HP Director's online account on February 1, 2006.

22. Another call was made to customer service on March 1, 2006. The CSR noted that the caller had the customer's social security number but not the mobile telephone number. The CSR then called the customer's number and determined that the customer's voicemail did not match the caller's voice. The CSR then updated the warning that was already in place on the account.

23. A final call to customer service occurred on March 14, 2006. The caller posed as a Verizon Wireless employee and requested information on the account. When the CSR stated that she would not provide any information, the caller hung up.

24. These three calls to customer service in February and March, and the online access to the account shortly after the February 2 call, all provide evidence that Defendants may have gained unauthorized access to the account of the HP Director's spouse.

The Harm Caused by Defendants

25. On information and belief, Defendants continue to offer unlawful pretexting services. Unless they are immediately restrained and enjoined from doing so, they will continue to engage in wrongful conduct to the detriment of Verizon Wireless and its customers. Moreover, Defendants' abuse of the customer service operations of Verizon Wireless detracts from the service provided to legitimate customers with genuine inquiries.

26. Defendants have not obtained authorization to access Verizon Wireless' customer accounts from Verizon Wireless, from Verizon Wireless' customers, or through duly issued subpoenas or court orders. Thus, Defendants cannot lawfully access Verizon Wireless' protected computers or customer accounts to obtain confidential customer information.

27. Verizon Wireless has been forced to expend resources, in excess of $5,000.00 for

each individual Defendant, in investigating the fraudulent activities associated with Defendants' unauthorized access to online customer accounts, and in remediating its systems and its customer relationships.

28. Verizon Wireless has been irreparably harmed in a number of ways by Defendants' unscrupulous practices pursuant to which Verizon Wireless' CSRs and/or computer systems have been caused to provide information to unauthorized individuals, including the following:

A. Defendants' actions invade the privacy of Verizon Wireless' customers;

B. Verizon Wireless' reputation has been harmed and the goodwill associated with it has been tarnished to a degree and extent that is not quantifiable and therefore not compensable with monetary damages; and

C. Verizon Wireless' customer service operations have been compromised by Defendants' deception of its CSRs and abuse of its systems.

29. Verizon Wireless thus brings this action: (a) to obtain temporary and permanent injunctive relief prohibiting any further attempts to improperly obtain customer information; (b) to seek replevin of all of Verizon Wireless' customer information in the possession of Defendants, regardless of the form or manner of storage, including without limitation Verizon Wireless' customer information existing on Defendants' computers and hard drives; (c) to obtain from Defendants the identities of their customers, and all persons or entities to whom they have communicated or transferred any Verizon Wireless customer information; (d) to seek an order requiring Defendants to account for and to disgorge all profits obtained as a result of their fraud and/or conversion of Verizon Wireless' confidential customer information; (e) to compensate Verizon Wireless for the damages caused by Defendants' illegal and/or fraudulent conduct; and

(f) to obtain such other and further relief as the Court deems equitable and appropriate, including costs and/or attorney's fees as directed by law.

COUNT ONE
(The Computer Fraud and Abuse Act, 18 U.S.C. § 1030)

30. Verizon Wireless hereby incorporates by reference and realleges each and every allegation of the prior paragraphs of the Complaint as if set forth completely herein.

31. Verizon Wireless owns and maintains certain "protected computers" within the meaning of 18 U.S.C. § 1030 (e)(2). These protected computers consist of high-speed data processing devices performing storage functions that are used in interstate or foreign commerce or communication or which affect interstate or foreign commerce and communication. These protected computers contain confidential customer information associated with Verizon Wireless customers.

32. Defendants intentionally accessed Verizon Wireless's computers without authorization, causing damage by impairing the integrity of Verizon Wireless's data and its online account services through the unauthorized creation or access of online customer accounts containing false and inaccurate information, in violation of 18 U.S.C. § 1030(a)(5)(A)(iii).

33. By way of conduct involving interstate communication, Defendants intentionally accessed Verizon Wireless's computers without authorization and thereby obtained information from a protected computer in violation of 18 U.S.C. § 1030(a)(2)(C).

34. Defendants also knowingly and with intent to defraud accessed Verizon Wireless's protected computers without authorization and data thereon was altered, thereby obtaining access to something of value – namely, the confidential customer information associated with the Verizon Wireless account – in violation of 18 U.S.C. § 1030(a)(4)computers were .

35. As a result of the conduct described above, each of the Defendants caused loss to Verizon Wireless during the past year aggregating at least $5,000 in value, in violation of 18 U.S.C. § 1030(5)(B)(i).

COUNT TWO
(Computer Related Offenses Act, N.J.S.A. 2A:38A-1)

36. Verizon Wireless hereby incorporates by reference and realleges each and every allegation of the prior paragraphs of the Complaint as if set forth completely herein.

37. The Defendants, purposefully or knowingly and without authorization, accessed, or attempted to access, Verizon Wireless's computer system or computer network.

38. The Defendants, purposefully or knowingly, accessed and obtained data from Verizon Wireless's computers, in violation of the Computer Related Offenses Act.

39. Verizon Wireless has been damaged in its business or property as a result of the Defendants' foregoing conduct.

COUNT THREE
(Fraud)

40. Verizon Wireless hereby incorporates by reference and realleges each and every allegation of the prior paragraphs of the Complaint as if set forth completely herein.

41. By calling Verizon Wireless' CSRs and pretending to be Verizon Wireless employees and customers, Defendants, by and through their employees and agents, have made numerous false statements of fact.

42. By accessing Verizon Wireless' computer systems and providing confidential customer details to Verizon Wireless to bypass security measures and either establish or access online accounts of Verizon Wireless customers without the authority to do so, Defendants, by and through their employees and agents, have made numerous false statements of fact.

43. These statements were known by Defendants to be false when made.

44. Defendants intended Verizon Wireless to rely on these statements.

45. Defendants have acted willfully, wantonly, and with malice.

46. Verizon Wireless has reasonably relied upon Defendants' false statements, and has been irreparably harmed and damaged as a result.

47. Defendants' actions constitute an actionable fraud.

48. If Defendants are not enjoined, Defendants will continue to engage in fraudulent conduct, causing irreparable harm to Verizon Wireless.

49. Because Defendants have acted willfully, wantonly, and with malice, Defendants should provide an accounting for, and should be ordered to disgorge, any and all profits wrongfully obtained as a result of their fraud.

50. Because Defendants have acted willfully, wantonly, and with malice, Verizon Wireless is entitled to punitive damages in an amount sufficient to deter Defendants from engaging in similar conduct in the future.

COUNT FOUR
(Conversion)

51. Verizon Wireless hereby incorporates by reference and realleges each and every allegation of the prior paragraphs of the Complaint as if set forth completely herein.

52. On information and belief, Defendants have received and are in possession of Verizon Wireless' customer information to which they are not entitled.

53. By commercially utilizing Verizon Wireless' confidential customer information and providing it to third parties, Defendants wrongfully have exercised dominion and control over Verizon Wireless' property, thereby depriving Verizon Wireless of its ownership interest. Defendants are not entitled to use Verizon Wireless' property in any way.

54. Such actions constitute a conversion of property rightfully belonging to Verizon Wireless.

55. Defendants have acted willfully, wantonly, and with malice.

56. As a direct and proximate result of Defendants' conduct, Verizon Wireless has suffered irreparable harm and damages in an amount to be proved at trial.

57. Unless they are enjoined, Defendants will continue to convert Verizon Wireless' confidential customer information and thereby cause irreparable harm to Verizon Wireless.

58. Because Defendants have acted willfully, wantonly, and with malice, Defendants should provide an accounting for, and should be ordered to disgorge, any and all profits wrongfully obtained as a result of their conversion of Verizon Wireless' confidential customer information.

59. Because Defendants have acted willfully, wantonly, and with malice, Verizon Wireless is entitled to punitive damages in an amount sufficient to deter Defendants from engaging in similar conduct in the future.

COUNT FIVE
(Unfair Competition and Trade Practices)

60. Verizon Wireless hereby incorporates by reference and realleges each and every allegation of the prior paragraphs of the Complaint as if set forth completely herein.

61. Defendants' behavior constitutes an unconscionable act and practice, and an unfair and deceptive act and practice, in the conduct of trade and commerce.

62. Verizon Wireless has expended millions of dollars every year to protect Verizon Wireless' confidential customer information.

63. Defendants have engaged in a course of conduct that is intentionally and foreseeably calculated to undermine and/or destroy Verizon Wireless' rights to fully benefit from

its ownership rights in and to Verizon Wireless' confidential customer information.

64. Defendants intended thereby to seize the value of Verizon Wireless' confidential customer information for its own benefit and indirectly for the benefit of its clients.

65. In furtherance of its scheme of unfair competition, Defendants have engaged in the following conduct:

A. Misappropriating Verizon Wireless' confidential customer information;

B. Violating confidentiality provisions between Verizon Wireless and its subscribers;

C. Inducing and encouraging others to violate confidentiality provisions and to misappropriate Verizon Wireless' confidential customer information;

D. Using deceptive means and practices in dealing with Verizon Wireless; and

E. Other methods of unlawful and/or unfair competition.

66. Defendants have acted willfully, wantonly, and with malice.

67. Unless they are enjoined, Defendants will continue to cause Verizon Wireless irreparable harm.

68. As a result of Defendants' behavior, Verizon Wireless has been irreparably harmed and damaged.

COUNT SIX
(Civil Conspiracy)

69. Verizon Wireless hereby incorporates by reference and realleges each and every allegation of the prior paragraphs of the Complaint as if set forth completely herein.

70. Upon information and belief, in connection with the foregoing actions, Defendants have entered into agreements or confederations with each other and third parties with

a common design to engage in an unlawful purpose of converting confidential Verizon Wireless customer information, through fraud and/or other unlawful means, which agreement has caused Verizon Wireless to suffer irreparable harm and damages.

71. Defendants have acted willfully, wantonly, and with malice.

72. In engaging in the foregoing conduct, one or more of the Defendants have engaged in overt acts in furtherance of the conspiracy, which have been the actual and proximate cause of damage to Verizon Wireless.

COUNT SEVEN
(Replevin)

73. Verizon Wireless hereby incorporates by reference and realleges each and every allegation of the prior paragraphs of the Complaint as if set forth completely herein.

74. Defendants have unlawfully received and unlawfully possess Verizon Wireless' customer information to which they are not entitled.

75. The property consists of any confidential information pertaining to Verizon Wireless' customers and recorded in written form by Defendants, including but not limited to the customers' names, home addresses, calling records, billing addresses, billing records, and telephone numbers. The value of Verizon Wireless' property is immeasurable and is difficult to ascertain with certainty.

76. The property has not been taken under an execution or attachment against Verizon Wireless' property.

77. Verizon Wireless is entitled to immediate possession of its customer information as the rightful owner of the property and because Defendants are engaging in conduct that places the confidential information in danger of improperly being used, copied, sold, or otherwise disclosed to third parties.

78. Verizon Wireless is entitled to replevin of all of its customer information in the possession of the Defendants, regardless of form or manner of storage, including without limitation Verizon Wireless' customer information existing on Defendants' computers and hard drives.

WHEREFORE, Verizon Wireless prays that judgment be entered in its favor and against Defendants as follows:

(a) That Defendants and any of their directors, officers, agents, servants, and employees, and those persons and entities in active concert or participation with them, be preliminarily and permanently enjoined from:

(i) attempting, directly or indirectly, to obtain any information from Verizon Wireless regarding any of Verizon Wireless' customers;

(ii) using the name or identity of any Verizon Wireless employee or customer for any purpose;

(iii) contacting Verizon Wireless for the purpose of obtaining confidential customer information , whether in person, over the phone, or online;

(iv) providing any Verizon Wireless customer information currently in their possession to any third parties;

(v) advertising that Defendants can or will obtain information regarding wireless telephone subscribers, including but not limited to making such representations on any website; and

(vi) possessing any confidential customer information obtained from Verizon Wireless, regardless of form or manner of storage.

(b) That Defendants be ordered to return to Verizon Wireless all confidential Verizon

Wireless customer information in their possession, regardless of the form or manner of storage, including all copies of such information;

(c) That Defendants be required to account for and to disgorge all profits obtained as a result of their fraud and/or conversion of Verizon Wireless' confidential customer information;

(d) That Defendants be ordered to pay Verizon Wireless compensatory and punitive damages, the cost of the suit, including a reasonable attorney's fee, and the costs of investigation and litigation, together with interest thereon; and

(e) That Verizon Wireless be granted such other and further legal and equitable relief against Defendants as the Court deems appropriate, including (i) an accounting of each and every person or entity a) whose confidential customer information was obtained, and b) that has been provided with Verizon Wireless' confidential customer information; and (ii) an award of costs and attorneys' fees.

Respectfully submitted,

GREENBERG TRAURIG, LLP

By: _____

Philip R. Sellinger (PS 9369)
Ian S. Marx (IM 1704)
200 Park Avenue
P.O. Box 677
Florham Park, New Jersey 07932-0677
(973) 360-7900 (Phone)
(973) 301-8410 (Facsimile)
Attorneys for Plaintiff
Cellco Partnership d/b/a Verizon Wireless

Dated: September 28, 2006

JURY DEMAND

Verizon Wireless demands a jury trial pursuant to Rule 38(b) of the Federal Rules of Civil Procedure for all issues so triable.

GREENBERG TRAURIG, LLP

By: _____

Philip R. Sellinger (PS 9369)
Ian S. Marx (IM 1704)
200 Park Avenue
P.O. Box 677
Florham Park, New Jersey 07932-0677
(973) 360-7900 (Phone)
(973) 301-8410 (Facsimile)
Attorneys for Plaintiff
Cellco Partnership d/b/a Verizon Wireless

Dated: September 29, 2006

CERTIFICATION PURSUANT TO L. CIV. R. 11.2

Pursuant to Local Civil Rule 11.2, I hereby certify that the within action is not the subject of any other action pending in any Court, or of any pending arbitration or administrative proceeding.

GREENBERG TRAURIG, LLP

By: _____

Philip R. Sellinger (PS 9369)
Ian S. Marx (IM 1704)
200 Park Avenue
P.O. Box 677
Florham Park, New Jersey 07932-0677
(973) 360-7900 (Phone)
(973) 301-8410 (Facsimile)
Attorneys for Plaintiff
Cellco Partnership d/b/a Verizon Wireless

Dated: September 14, 2006

CERTIFICATION PURSUANT TO LOCAL CIVIL RULE 201.1(d)(3)

Pursuant to Local Civil Rule 201.1(d)(3), I hereby certify that the damages recoverable in this action exceed the sum of $150,000, exclusive of interest and costs and any claim for punitive damages.

GREENBERG TRAURIG, LLP

By: _____

Philip R. Sellinger (PS 9369)
Ian S. Marx (IM 1704)
200 Park Avenue
P.O. Box 677
Florham Park, New Jersey 07932-0677
(973) 360-7900 (Phone)
(973) 301-8410 (Facsimile)
Attorneys for Plaintiff
Cellco Partnership d/b/a Verizon Wireless

Dated: September 29, 2006

VERIFICATION

STATE OF CALIFORNIA)
) ss.
COUNTY OF _____)

KAREN MINK, being duly sworn, deposes and says:

I am an Investigator within the Security Department of Cellco Partnership d/b/a Verizon Wireless ("Verizon Wireless"), the plaintiff herein. I have read the foregoing Complaint and know the contents thereof, and believe that the same are true, based upon my own knowledge, my review of Verizon Wireless's business records and conversations, except as to the matters stated to be alleged upon information and belief, and as to those matters I believe them to be true.

I verify under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Karen Mink
KAREN MINK

Sworn to before me this
____ day of September, 2006

_____
Notary Public

State of California County of
CONTRA COSTA
Subscribed and sworn to (or affirmed)
Before me on this 27th day of SEP 2006 by
KAREN LYNN MINK
personally known to me or proved to me on
the basis of satisfactory evidence to be the
person(s) who appeared before me.
Signature Lahamber Singh Dhanda
(Seal)

LAHAMBER SINGH DHANDA
Commission # 1576444
Notary Public - California
Contra Costa County
My Comm. Expires May 6, 2009

EXHIBIT 1

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549-1004

FORM 8-K

CURRENT REPORT

PURSUANT TO SECTION 13 OR 15(d) OF
THE SECURITIES EXCHANGE ACT OF 1934

August 31, 2006
Date of Report (Date of Earliest Event Reported)

HEWLETT-PACKARD COMPANY
(Exact name of registrant as specified in its charter)

DELAWARE	**1-4423**	**94-1081436**
(State or other jurisdiction of incorporation)	(Commission File Number)	(I.R.S. Employer Identification No.)

3000 HANOVER STREET, PALO ALTO, CA	**94304**
(Address of principal executive offices)	(Zip code)

(650) 857-1501
(Registrant's telephone number, including area code)

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions:

☐ Written communications pursuant to Rule 425 under the Securities Act (17 CFR 230.425)

☐ Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)

☐ Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))

☐ Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

Item 8.01. Other Events.

On May 22, 2006, Hewlett-Packard Company ("HP") announced the resignation of Thomas J. Perkins from its Board of Directors. At the time of his resignation, Mr. Perkins did not provide any written communication to HP concerning the reasons for his resignation. Following his resignation, and after HP on May 22 had disclosed the fact of Mr. Perkins' resignation on Form 8-K in accordance with the applicable federal securities laws, Mr. Perkins notified HP that he had concerns with the HP Board's handling of investigations that had been conducted into leaks of confidential HP information from meetings of the HP Board of Directors. HP is filing this Form 8-K to report the following additional information about the circumstances relating to Mr. Perkins' resignation, to report the findings of its leak investigations, and to report other related events that have occurred subsequent to the completion of those investigations and Mr. Perkins' resignation.

HP has been the subject of multiple leaks of confidential HP information, including information concerning the internal deliberations of its Board of Directors. HP believes these leaks date back to at least 2005. In response to these leaks, outside legal counsel conducted interviews of directors in early 2005 in order to determine the source of the leaks and to obtain each director's reaffirmation of his or her duty of confidentiality. The interview process did not yield the source of the leaks. Notwithstanding these actions, the leaks continued. As a result, the Chairman of the Board, and ultimately an internal group within HP, working with a licensed outside firm specializing in investigations, conducted investigations into possible sources of the leaks of confidential information at HP. Those investigations resulted in a finding that Dr. George A. Keyworth II, one of HP's directors, did, in fact, disclose Board deliberations and other confidential information obtained during Board meetings to the media without authorization. At a Board meeting on May 18, 2006, after Dr. Keyworth acknowledged that he had leaked confidential information, the Board, after deliberation, asked Dr. Keyworth to resign his position as a director, which he declined to do. It is at that meeting that Mr. Perkins resigned from the Board after expressing personal frustration with the Chairman of the Board relating to the handling of the matter with the Board. He stated that he objected to the matter being brought before the full Board and that he believed the Chairman had agreed that he and she would handle the matter privately. The Chairman disputed Mr. Perkins' assertion, explaining that she was complying with advice from outside counsel on the appropriate handling of the matter. At the time, Mr. Perkins confirmed he did not have any disagreement with HP on any matter relating to HP's operations, policies or practices.

On June 19, following his resignation and after HP reported Mr. Perkins' resignation on Form 8-K, Mr. Perkins sought information from HP concerning the methods used to conduct HP's investigations into the leaks, asserted that phone and e-mail communications had been improperly recorded as part of the investigation, and informed HP that he had recently consulted with counsel regarding that assertion. In response to Mr. Perkins' request, HP informed Mr. Perkins that no recording or eavesdropping had occurred, but that some form of "pretexting" for phone record information, a technique used by investigators to obtain information by disguising their identity, had been used. Mr. Perkins, although no longer a director, then requested that HP conduct an inquiry into the propriety of the techniques used to conduct the investigation.

HP's Nominating and Governance Committee thereafter engaged the outside counsel to conduct an inquiry into the conduct and processes employed with respect to HP's investigation of leaks of

confidential information (the outside counsel was not involved in the investigations of the leaks initiated by the Chairman or the internal HP group). The Committee was advised that HP had engaged an outside consulting firm with substantial experience in conducting internal investigations and that this firm had retained another party to obtain phone information concerning certain calls between HP directors and individuals outside of HP. The Committee was further advised that the Chairman and HP had instructed the outside consulting firm to conduct its investigation in accordance with applicable law and that the outside consulting firm and its counsel had confirmed to HP that its techniques were legal. After its review, the Committee determined that the third party retained by HP's outside consulting firm had in some cases employed pretexting. The Committee was then advised by the Committee's outside counsel that the use of pretexting at the time of the investigation was not generally unlawful (except with respect to financial institutions), but such counsel could not confirm that the techniques employed by the outside consulting firm and the party retained by that firm complied in all respects with applicable law.

Based upon its investigation, the Nominating and Governance Committee has recommended to HP's Board and Chief Executive Officer that controls relating to investigations be strengthened and that management should be in a position to assure that all aspects of HP's investigations comply with applicable laws and HP's code of ethics as applicable to HP's directors, officers and employees. HP's Board and Chief Executive Officer have accepted the conclusions and recommendations of the Committee.

HP recently has been informally contacted by the Attorney General of the State of California requesting information concerning the processes employed in the investigations into the leaks. HP intends to cooperate fully with that inquiry. HP also has received a comment letter from the staff of the Securities and Exchange Commission's Division of Corporation Finance with respect to its May 22 Form 8-K regarding Mr. Perkins' resignation. HP intends to respond to the SEC staff that it believes its disclosures in the May 22 Form 8-K with respect to Mr. Perkins' resignation were accurate and complete at the time of filing and were based upon Mr. Perkins' actions and representations prior to such time concerning the reasons for his resignation.

In addition, on August 31, 2006 the HP Board of Directors, upon the recommendation of the Nominating and Governance Committee, also determined that, based on his conduct, Dr. Keyworth should not be nominated for another term on the Board of Directors.

SIGNATURE

Pursuant to the requirements of the Securities Exchange Act of 1934, the registrant has caused this report to be signed on its behalf by the undersigned hereunto duly authorized.

HEWLETT-PACKARD COMPANY

DATE: September 6, 2006

By: /s/ Charles N. Charnas
Name: Charles N. Charnas
Title: Vice President, Deputy General Counsel and Assistant Secretary

EXHIBIT 2

1 of 1 DOCUMENT

The New York Times

September 8, 2006 Friday
Correction Appended
Late Edition - Final

SECTION: Section C; Column 6; Business/Financial Desk; Pg. 1

LENGTH: 1025 words

HEADLINE: H.P. Spied On Writers In Leaks

BYLINE: By DAMON DARLIN

DATELINE: SAN FRANCISCO, Sept. 7

BODY:

The California attorney general's investigation into the purloining of private phone records by agents of Hewlett-Packard has revealed that the monitoring effort began earlier than previously indicated and included journalists as targets.

The targets included nine journalists who have covered Hewlett-Packard, including one from The New York Times, the company said.

The company said this week that its board had hired private investigators to identify directors leaking information to the press and that those investigators had posed as board members -- a technique known as pretexting -- to gain access to their personal phone records.

In acknowledging Thursday that journalists' records had also been obtained, the company said it was apologizing to each one. "H.P. is dismayed that the phone records of journalists were accessed without their knowledge," a company spokesman, Michael Moeller, said.

In an interview Thursday about the state's criminal investigation of the Hewlett-Packard matter, Attorney General Bill Lockyer said, "A crime was committed." But he added: "It is unclear how strong the case is. Who is charged and for what is still an open question."

Mr. Lockyer said search warrants would be issued to obtain the records of Internet service providers in an attempt to trace the identities of the imposters. He said Hewlett-Packard was cooperating with the investigation into what he said was the first California case of a major corporation using such methods to obtain phone records.

An investigator with direct knowledge of the state's inquiry characterized the list of targets as "extensive," though that person would not elaborate. It could contain people other than journalists or directors.

Travis Dodd, general attorney with AT&T Services in San Antonio, who is working with the California prosecutors, said the records of John Markoff, a reporter for The Times in San Francisco, were a "target of the pretexting" in 2005.

Two other news organizations, the online technology news service CNET and The Wall Street Journal, said they had learned that their reporters had also been targets.

A top Hewlett-Packard official indicated earlier this week that the effort to obtain phone records had begun in January 2006 after an article appeared on CNET with accounts of a Hewlett-Packard management meeting. Those reve-

lations prompted H.P.'s chairwoman, Patricia C. Dunn, to order an investigation of leaks, and the company has conceded that subterfuge was used by a subcontractor to gain phone records in the investigation.

Hewlett-Packard has refused to publicly disclose the names of the consulting firm it hired or the subcontractor that was used to pretext the records. The company has said that the outside consulting firm was instructed to conduct its investigation according to law and that the firm had told H.P. that its techniques were legal.

In May, that investigation identified the board's longest-serving member, George A. Keyworth II, as the source of the leak. He rebuffed a request to resign, but the company said he would not be renominated. Thomas J. Perkins, another board member, resigned in anger over the way the investigation was conducted. His efforts to get the company to acknowledge the reason for his departure led to this week's disclosures.

There had been earlier concerns at the company about leaks around the time of Carleton S. Fiorina's dismissal as chief executive in early 2005. An investigation at that time, however, was only known to have involved interviews of board members.

Viet D. Dinh, Mr. Perkins's lawyer, said Thursday, "If it is true that the pretexting started before January 2006 and dated back to 2005, it would suggest a deeper and more troubling chain of events than the hiring of third-party pretexters and would reach much higher to persons responsible at H.P."

By Mr. Perkins's account, only the law firm of Wilson Sonsini Goodrich & Rosati, a powerful Silicon Valley law firm and outside counsel for Hewlett-Packard, conducted investigations into leaks in 2005.

A spokeswoman for the law firm, Courtney Dorman, said the firm "absolutely, definitely did not" use pretexting or hire anyone who did pretexting during the firm's informal investigation of directors in 2005.

Mr. Moeller said Thursday that the company's statements about the pretexting had never confined those events to 2006.

A lawyer for The New York Times, David McCraw, said on Thursday evening, "We are deeply concerned by reports that the rights of one of our reporters were violated."

"To the extent that this is a criminal matter, we will cooperate with authorities to make sure any wrongdoing is prosecuted," he said. "To the extent it is a civil matter, we will pursue whatever legal recourse is available. We expect as an initial step that H.P. will make a prompt and full disclosure of what took place in regards to our reporter."

CNET said Thursday that phone records of one of its reporters, Dawn Kawamoto, had also been obtained. A spokeswoman, Sarah Cain, said: "These actions not only violated the privacy rights of our employee, but also the rights of all reporters to protect their confidential sources."

CNET said access to Ms. Kawamoto's records had been gained from the same Internet address used by the person who accessed the phone records of Mr. Perkins. A caller used the last four digits of her husband's Social Security number to establish an online account with AT&T to view the records. Access was gained on one date, in late January 2006, it said.

An article in The Wall Street Journal said records of its reporter, Pui-Wing Tam, had also been a target of pretexting activity. A spokesman for Dow Jones, owner of The Wall Street Journal, declined to comment.

Investor reaction to the Hewlett-Packard board furor has been muted. The company's stock closed Thursday at $35.42, down 2.85 percent from its close before news of the board's turmoil was reported. Indeed, at a Citigroup investor conference where Mark V. Hurd, the chief executive, spoke and answered questions Wednesday, no securities analyst asked about the problems.

URL: http://www.nytimes.com

CORRECTION-DATE: September 9, 2006

CORRECTION:

An article in Business Day yesterday about the purloining of private phone records in a Hewlett-Packard investigation of news leaks misattributed a disclosure that a reporter for The New York Times, John Markoff, was a target of the effort. The information came from the California attorney general's office, not a lawyer for AT&T.

LOAD-DATE: September 8, 2006

EXHIBIT 3

1 of 1 DOCUMENT

The New York Times

September 18, 2006 Monday
Late Edition - Final

SECTION: Section A; Column 5; National Desk; Pg. 1

LENGTH: 1834 words

HEADLINE: Hewlett Review Is Said to Detail Deeper Spying

BYLINE: By DAMON DARLIN; Kurt Eichenwald contributed reporting.

BODY:

A secret investigation of news leaks at Hewlett-Packard was more elaborate than previously reported, and almost from the start involved the illicit gathering of private phone records and direct surveillance of board members and journalists, according to people briefed on the company's review of the operation.

The effort received some degree of supervision from three officials -- Patricia C. Dunn, the company's chairwoman, along with its general counsel and another staff attorney -- but was quickly farmed out to a network of private investigative firms early last year, according to descriptions of the findings. It is still unclear how much they knew of the details.

Those briefed on the company's review of the operation say detectives tried to plant software on at least one journalist's computer that would enable messages to be traced, and also followed directors and possibly a journalist in an attempt to identify a leaker on the board.

The revelations at Hewlett-Packard, the computer and printer maker that helped define Silicon Valley, have provided a rare glimpse of boardroom turmoil -- resulting in Ms. Dunn's agreement to step down as chairwoman in January, and two resignations from the board.

But they have also cast a harsh light on the questionable and possibly illegal techniques used in the episode, raising the possibility of criminal charges.

The account of those briefed on Hewlett-Packard's review of the matter sheds new light on the scope and timing of the investigative methods, establishing that invasive and possibly illegal techniques were used far earlier than previously known and that the company's chief ethics officer was among those providing supervision.

The hunt for a boardroom leaker began as early as January 2005, with a focus on disclosures immediately preceding the ouster of Carleton S. Fiorina as chairwoman and chief executive, with a second phase that began a year later. Hewlett-Packard has said that as a public company, it had a responsibility to stop unauthorized disclosures.

But the review reveals that the investigation by its detectives was notable for a lack of close supervision by company officials.

Those briefed on the internal review said that at various times, questions were raised about the legality of the methods used. They did not identify who raised the questions, when, or to whom they were addressed. But a crucial legal opinion, its origins previously undisclosed, was supplied by a Boston firm that shares an address and phone number with a detective firm on the case.

Those speaking about the company's review would do so only if they were not identified. A Hewlett-Packard spokesman yesterday declined to comment on their account.

In addition to scrutiny by prosecutors, a House subcommittee has entered the case, asking for documents on the internal investigation to be delivered today in advance of a Sept. 28 hearing in Washington.

Some of those documents are expected to reveal that detectives made several attempts at direct surveillance of some directors, and were given photos of reporters to help identify them.

At least one reporter, Dawn Kawamoto of the online technology news service CNET, may have been followed as part of the 2006 investigation, said a person briefed on the investigation. Ms. Kawamoto was a co-author of an article on a senior management meeting in January.

The detectives also tried to plant software in the computer of an unspecified CNET reporter that would communicate back to the detectives, people briefed on the company review said. Ms. Kawamoto said in an interview this month that prosecutors had told her that such a ploy may have been used, but said she was not aware of any surveillance.

Representing themselves as an anonymous tipster, the detectives e-mailed a document to a CNET reporter, according to those briefed on the review. The e-mail was embedded with software that was supposed to trace who the document was forwarded to. The software did not work, however, and the reporter never wrote any story based on the bogus document.

On Saturday, the company identified one of two employees who it said had been a target of scrutiny in the internal operation. It said the private phone records of the employee, Michael Moeller, director of corporate media relations, were taken.

It is not clear why Mr. Moeller, whose job it is to speak with reporters, was included in the operation. Robert Sherbin, Hewlett-Packard's vice president for external communications and Mr. Moeller's boss, said yesterday, "Investigators' suspicions were misdirected and were unfounded." He would not elaborate.

Although the company said others outside the company were also targets of detectives, it has not identified those people.

According to those briefed on the internal review, the Hewlett-Packard investigation had two stages: from January to August 2005, when nothing of substance was turned up, and again in January 2006, after the CNET article appeared.

The first call for an investigation from the board came in January 2005 after The Wall Street Journal published an article that cited discussion of the board about a management reorganization and changes in the responsibilities of Ms. Fiorina, then chairwoman and chief executive.

An article in The New York Times on Feb. 10, recounting Ms. Fiorina's ouster by the board, contained extensive details of a directors' meeting and fueled the desire to plug leaks.

Reporters from those two newspapers, CNET and Business Week have been told by the California attorney general's office that they were targets in the operation.

Within 60 days, the investigation into the leaks was up and running, according to those briefed on the company review. Responsibility for the investigation was delegated to the company's global investigations unit, based in the Boston area. Those company officials turned the effort over to Security Outsourcing Solutions, a two-person agency that hires specialists for investigations.

That firm hired Action Research Group, an investigative firm in Melbourne, Fla. The actual work of obtaining the phone records was given to other subcontractors, one of which is said to have worked in or near Omaha. The methods were said to have included the use of subterfuge, a practice known as pretexting, in which investigators pose as those whose records they are seeking.

Previous accounts of the Hewlett-Packard operation have focused on the use of such methods in the 2006 phase of the investigation, but not in its earlier phase.

Federal and California prosecutors, as well as the Congressional subcommittee, are examining the chain of detectives for possible criminal wrongdoing in obtaining phone records. The California attorney general said last week that he had enough evidence to indict people inside and outside the company.

Hewlett-Packard has steadfastly refused to identify any of the investigators it used, including its own.

People briefed on Hewlett-Packard's review of its internal investigation say that it was authorized by Ms. Dunn, the chairwoman, and put under the supervision of Kevin Hunsaker, a senior counsel who is the company's director of ethics. But it is not clear what level of supervision he gave to the project.

Ms. Dunn has said in recent interviews that she could not supervise the investigation because she was also a potential target. She has said she turned to the company's security department in April or May 2005 for an initial investigation, then asked Ann O. Baskins, the company's general counsel, for help in the further investigation last January. Ms. Baskins supervises a team of more than 100 lawyers around the world.

At at least one point, the company's lawyers sought a legal opinion. But it did not come from Hewlett-Packard's own outside counsel, Larry W. Sonsini of Wilson Sonsini Goodrich & Rosati, an eminent Silicon Valley law firm.

Instead, the company asked one of its contractors, Security Outsourcing Solutions, which turned to a Boston lawyer, John Kiernan of Bonner Kiernan Trebach & Crociata, for the opinion. Mr. Kiernan's office shares a Boston address and phone number with Security Outsourcing Solutions.

The company, in a recent filing with the Securities and Exchange Commission, said it had received an outside counsel's opinion that the investigative methods were legal, but it did not identify the source.

It is also not clear whether company lawyers were aware of the close business and personal ties between Mr. Kiernan, Ronald R. DeLia, the owner of Security Outsourcing Solutions, and Anthony R. Gentilucci, the Boston-based manager of global investigations for Hewlett-Packard.

Executives and lawyers back in the company's Palo Alto, Calif., headquarters remained in the dark even after a summary report was produced for them about each of the two phases of the operation, according to those briefed on the review. Neither of the reports, they said, outlined the methods used.

There were discussions of phone numbers and calls in the report. But it is not clear why that fact apparently did not raise alarm among any Hewlett-Packard lawyers about the means used to gain the information.

The findings were presented to the board at a meeting in May, with George A. Keyworth II, the board's longest-serving member, identified as a source of leaks. He refused an initial request to resign, though he ultimately agreed to do so last week. But a fellow director, Thomas J. Perkins, a Silicon Valley venture capitalist, resigned immediately over the handling of the investigation.

It was only through subsequent inquiries to Mr. Sonsini that Mr. Perkins learned more about the methods used. It was his determination to get the company to acknowledge the reasons for his departure that brought the internal investigation into the spotlight this month.

In an e-mail message to Mr. Sonsini on June 19 , Mr. Perkins asked about the legality of obtaining private phone records without a subpoena. Mr. Sonsini responded that Ms. Baskins had "looked into the legality of every step of the inquiry and was satisfied that it was conducted properly."

According to those briefed on the company's review of its investigation, there is no indication that Mr. Sonsini, considered the most powerful lawyer in Silicon Valley, was involved in seeking outside investigators for Hewlett-Packard in 2005 or 2006. He became involved, they said, only when the board asked him for a legal opinion of the investigation and the methods used.

Mr. Sonsini has said that his direct involvement in helping the board trace news leaks was limited to interviews with directors in early 2005.

Mr. Sonsini told the board in August, after his firm's investigation of the detectives' methods, that the use of pretexting "was not generally unlawful." The law firm could not say whether the detective agencies hired by Hewlett-Packard, or the subcontractors any of them used, "complied in all respects with applicable law."

URL: http://www.nytimes.com

GRAPHIC: Photos: Hewlett-Packard's chairwoman, Patricia C. Dunn, top, and general counsel, Ann Baskins, were said to have provided some supervision of a secret investigation of board members and journalists. (Photo by Hewlett-Packard via Bloomberg News)

(Photo by Paul Sakuma/Associated Press)(pg. A23)

LOAD-DATE: September 18, 2006

EXHIBIT 4

1 of 1 DOCUMENT

The New York Times

September 12, 2006 Tuesday
Late Edition - Final

SECTION: Section C; Column 2; Business/Financial Desk; Pg. 1

LENGTH: 983 words

HEADLINE: House Panel and U.S. Attorney Join H.P. Inquiry

BYLINE: By DAMON DARLIN

DATELINE: SAN FRANCISCO, Sept. 11

BODY:

As its directors continued to confer on the future of its chairwoman, Hewlett-Packard found itself under increased legal and political scrutiny Monday over the use of private investigators to trace the source of news leaks in the board.

The United States attorney's office in San Francisco said it was looking into the methods used by the investigators, which included the questionable if not illegal tactic of "pretexting" -- posing as directors and journalists to get their phone records.

The House Committee on Energy and Commerce, meanwhile, asked the company to identify the consulting firm it hired for the investigation, the subcontractor that carried out the ruses and all of the targets. It also demanded copies of contracts and legal opinions in the matter.

The company's board, which met inconclusively on Sunday, resumed telephone consultations Monday afternoon. Foremost among the topics was the role of the chairwoman, Patricia C. Dunn, who the company says first authorized the investigation last year.

Ms. Dunn recused herself from parts of the discussion, according to a person with knowledge of the board's deliberations, leaving the company's outside counsel, Larry W. Sonsini, chairman of the powerhouse Silicon Valley law firm of Wilson Sonsini Goodrich & Rosati, to preside.

Mr. Sonsini and his firm were consulted at various points in the investigation, according to the company. As a result, his role at the board meeting was "an odd choice," said Jeffrey A. Sonnenfeld, a professor at the Yale School of Management who advises companies on corporate governance. "They have a highly conflicted law firm right now," he said.

Hewlett-Packard spokesmen would not comment on the board's deliberations, and Mr. Sonsini has not responded to requests for comment since the upheaval at the company became public last week.

Over the weekend, in a reflection of the high stakes, Ms. Dunn brought in Sitrick & Company, a well-known and tenacious public relations firm specializing in crisis management, to represent her and the company. Michael S. Sitrick, the firm's chairman and chief executive, has represented a number of high-profile clients, including the supermarket billionaire Ronald W. Burkle when a contributor to The New York Post was accused of trying to extort money from him.

One reason for the board's extended talks was reported to be discussion of Thomas J. Perkins, who quit the board in May in anger at Ms. Dunn over the internal investigation. A person with knowledge of the board's deliberations said that Mr. Perkins, a pre-eminent Silicon Valley venture capitalist, sought to return to the board but that members are split on whether he should.

Mr. Perkins's spokesman, Mark Corallo, disputed that report. "Mr. Perkins will not return to the H.P. board, even if asked," Mr. Corallo said, but "he believes in the performance and prospects of the company under the leadership of Mark Hurd."

While Mr. Perkins has been an ally of Mark V. Hurd, the chief executive -- Mr. Perkins, like Mr. Hurd, sees H.P. as a growth company -- his public airing of his problems with Ms. Dunn has injured the company's image. (Hewlett-Packard's stock, though, has been relatively unscathed since the furor became public last week. It closed up slightly Monday at $36.36.)

Mr. Perkins's insistence that the company acknowledge his reason for resigning in May -- and his disclosure of what he had learned about the investigative tactics -- led to the current upheaval. He and his lawyer presented information to the federal authorities at the same time that they sent information to the California attorney general and the Securities and Exchange Commission, both of which have indicated they are already conducting inquiries.

Corporate governance experts are split over whether the board should ask Ms. Dunn to step down.

"This is one of the biggest corporate blunders in the past 10 years," said Charles M. Elson, director of the Weinberg Center for Corporate Governance at the University of Delaware. "To get this far off tells you that something was wrong with the board."

Mr. Sonnenfeld said the directors would be wise to keep the board's chairmanship separate from the chief executive position, if only because the chairman can "take the bullets" that might otherwise hit the chief executive. "It keeps Mark Hurd above the fray," Mr. Sonnenfeld said.

Removing Ms. Dunn, he said, will not make the problems go away, but will just shift the focus to Mr. Hurd, who sits on the board. "I wouldn't think he'd want to be in the chair right now," he said.

A big part of the company's problem is that it has been unwilling to speak out. Joseph A. Grundfest, a professor of law and business at Stanford Law School, said the company should be saying two things.

First, it needs to say that pretexting is wrong. "There hasn't been a clear, unambiguous message," he said. Saying that would allow the company to shift the terms of the debate, he said.

"Dunn was also pretexted," he said. "She was as much a victim."

He also said the focus should be on the leaker, George A. Keyworth II, a long-serving board member who was asked to resign but has refused. "This verges on the preposterous," Mr. Grundfest said, adding that he thought the company should even take legal action against him.

"Mr. Keyworth has said, 'You can't trust me, but share confidential company information with me,' " Mr. Grundfest said.

Another public battle may not be the most appealing prospect, but Ralph D. Ward, the publisher of Boardroom Insider, an online magazine on corporate governance, suggested that an outside panel was needed to evaluate the board. "Not Larry Sonsini," he said. "He seems to have been part of the problem."

The panel, composed of governance experts, might help to establish the board's credibility and independence, Mr. Ward said.

URL: http://www.nytimes.com

GRAPHIC: Photo: Mark V. Hurd, the chief executive of Hewlett-Packard, is also a member of the company's board. (Photo by Marcio Jose Sanchez/Associated Press)(pg. C8)

LOAD-DATE: September 12, 2006

EXHIBIT 5

Panel Adds 5 Investigators to HP Data Hearing

By REUTERS
Published: September 27, 2006

Filed at 1:42 p.m. ET

REUTERS

WASHINGTON (Reuters) - A U.S. House of Representatives panel on Wednesday extended its probe into Hewlett-Packard Co.'s (HPQ.N) use of private telephone records by subpoenaing five private investigators to testify at a Thursday hearing.

The investigators from Colorado, Georgia, Florida anfor the hearing and declined further comment.

Selvage, Preston and Brost could not immediately be reached for comment.

The unfolding HP scandal has revived legislation in the House and Senate that would set criminal penalties for pretexting and additional safeguards to protect the privacy of telephone records.