



UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF INNOVATION AND IMPROVEMENT

Dr. Matthew Goldstein, Chancellor
The City University of New York
The Chancellor's Office
535 E. 80th Street
New York, New York 10021

MAY 15 2005

Dear Dr. Goldstein:

This Office asked you by letter dated September 26, 2005, to investigate and respond to a report we received from a school official at the City University of New York (University or CUNY) about the unauthorized release of information from the education records of 335 law school students on September 21, 2005. As noted in our prior letter, under the Family Educational Rights and Privacy Act (FERPA), an educational agency or institution may not have a policy or practice of permitting the release of or providing access to education records, or personally identifiable information from education records, without the prior written consent of a parent or eligible student (as defined in § 99.3 of the regulations) except as authorized by law. 20 U.S.C. § 1232g(b)(1) and (b)(2); 34 CFR § 99.30, 99.31. We interpret this prohibition to mean that education records must be protected against unauthorized access and disclosure through the use of physical, technological, procedural or other security methods that are reasonable and appropriate to the circumstances in which the information is maintained. An agency or institution that leaves education records unprotected and subject to access by unauthorized individuals has not met this requirement.

Our September 26, 2005, letter explained that there was no evidence at that time that the security breach was a deliberate disclosure or due to the University's failure to take reasonable and appropriate steps to protect the education records it maintains. However, once the University became aware of the problem it was required to investigate the source of the breach and determine what steps, if any, should be taken to guard against the unauthorized disclosures that occurred. We noted further that the University was required to attempt immediately to retrieve the information and ensure that it was no longer being disclosed. Failure to take these steps could constitute a policy or practice of violating FERPA by permitting the disclosure of personally identifiable information from education records without the required prior written consent.

In order to ensure that the University remains in compliance with FERPA, our September 26, 2005, letter asked you to provide a written response to several questions, which are set forth below. Frederick P. Schaffer provided the University's response by letter dated October 27, 2005. Following is a summary of that response, which includes information from a report dated September 27, 2005, to the Board of Trustees by Brian Cohen, Chief Information Officer, and Barry Kaufman, University Controller, which Mr. Schaffer provided with his letter.

1. Describe the date, type and amount of information from education records that was disclosed without consent, including the number of students whose records were disclosed and the nature of any non-directory information that was released.

On September 21, 2005, the University discovered that a financial aid report containing the first and last names, social security numbers (SSNs), and amount of financial aid for 335 law students who had received checks from government loan programs in the September 14 distribution “had been posted on Google inadvertently.” Students who received private financial aid were not affected. (Chancellor Goldstein’s September 27, 2005, report to the Board of Trustees indicates that the security breach also involved records of 436 school employees, discussed briefly below.)

2. Explain how the information was disclosed through Google.

A student informed the Dean of Students Office that upon searching her name in Google “a link appeared to a central university website (which is referred to in the university as the ‘CUNY portal’.)” The link produced the entire list of CUNY law school students who received financial aid checks in the September 14, 2005, distribution. It was determined that this financial aid report resided on a “content server” located at the 555 West 57th Street Data Center

The University located the problem and closed access to the list on the CUNY portal by 6:00 p.m. on September 21. However, “confidential student information on the list remained accessible on Google even after the central University blocked access to the link.... by accessing Google’s stored HTML Cached content.” In the course of investigating the release of students’ financial aid records the University determined that sensitive information about certain school employees was also cached on Google servers and needed to be removed.

While the impact was the same for the law school students and the school employees whose records were released, the reasons for the breach were different. In regard to the student records, the University explained that “CIS [Computing and Information Services] established policies on protecting sensitive and confidential content were not strictly adhered to.” In particular,

When CIS is engaged to protect sensitive content, the report information is moved into an existing directory on a content server and a security policy is enabled to provide access to only authorized users. In the case of the Law School, the University Controller’s Office created the Law School directory and did not inform CIS of its existence or request security to be enabled.

September 27, 2005, report from Chief Information Officer and University Controller at page 2 (emphasis added). In regard to the records of school employees, “CIS created directories for each of the distinct colleges and campus schools. When security was enabled on these directories, errors were made in setting the policies for [these schools]. Testing by the Controller’s Office or CIS did not identify these errors.” Id. The report continues:

Assessment Risk: Review of the Controller’s (OUC) Office report directory structure and the existing security policies indicated that two sub-branches from the OUC directory were not protected by the CIS security policies: the School of Law and the Hunter

Elementary and High School report folders. Personal data, including name, social security number, and financial aid awards (335 Law School Students) or salary information (265 Active Hunter Elementary and High School employees; 171 Inactive Hunter Elementary and High School employees) were exposed to potential public access. No other sensitive information, such as banking or financial institution information was compromised.

While both directories had been indexed by a number of search engines, the only one that was found to contain cached content was Google. Google, as part of its standard practice, caches a copy of the indexed content on their servers.

Analysis of network logs indicates that from the period of 7/1/2005 – 9/22/2005 the Hunter Elementary and High School reports were accessed a total of 217 times; 180 were by the Google search engine alone. The Law School report folder was created in August 2005. Currently CIS is reviewing its logs to determine how many times this content has been accessed.

3. Describe what steps the University has taken to stop the continued release of this information through Google or otherwise.

University officials notified Google of the security breach on September 21, 2005, and asked them to remove the content. Google officials stated that cached content removal can take as much as 3-5 business days. The University escalated the matter to Google's corporate offices and, by 6:45 p.m. on September 23 (approximately 48 hours later), Google reported that the content was removed

Also on September 21, 2005, directory browsing of the CUNY Portal was disabled, and security policies were implemented for the OUC Root Directory at CUNY Law School to restrict access to the content. Central University and law school staff searched other portals or search engines, such as Yahoo, and found no other caches of this information. All remaining campus secured content links were checked to verify restricted access.

The University urged students who were notified not to discuss the security breach with anyone until after the information was removed from Google.

4. Describe what steps the University has taken to ensure that this kind of unauthorized release of information from education record does not occur in the future.

The University affirmed its commitment to a "policy and practice of safeguarding" education records and retained KPMG LLP for advice during its investigation of this security breach and to analyze any continuing computer system vulnerability. The University further committed to continue its investigation of this matter and to "make any changes necessary to ensure compliance." The University stated that it has taken the following "preventive actions" in response to this incident:

- A security policy has been implemented over the entire OUC content tree severely limiting potential exposure and preventing search engine access.
- The Controllers Office and CIS have reviewed procedures required to post sensitive content to the content servers that reside at the University's Data Center. Testing responsibilities have been established.
- CIS has revised its internal portal content policies requiring a one-to-one mapping of the security policies to the content update scripts. This change forces CIS participation whenever content distribution scope changes are required.
- The University has hired its first chief information security officer starting in October 2005.

According to Mr. Schaffer, on September 22, 2005, the University also notified all affected students of the "possible breach of confidential information" and advised them how to "protect themselves against possible fraudulent use of their personal information by notifying credit agencies and placing an initial fraud alert on credit reports." Students were provided with a copy of the Federal Trade Commission's Consumer Alert "What To Do If Your Personal Information Has Been Compromised." Senior administrators also met with students on September 27 to "explain what happened and help them take necessary steps to prevent any misuse of the information that was accessible."

It appears that the University reacted promptly to identify the cause of the unauthorized disclosure identified on September 21, 2005, and prevent any subsequent disclosures of this nature. We note, however, that the Office of the State Comptroller had previously expressed concerns about the University's methods for protecting its computer systems and data in Report 2003-S-10, General Controls at the Data Center and Selected Colleges (January 13, 2004). In connection with that audit, the University acknowledged that "the increased reliance on the use of IT systems brings increased security risks" and expressed its commitment to "formulating effective computer and network security and access controls in the management of our IT systems." December 1, 2003, letter from Louis Chiacchere to Office of the State Comptroller, available at www.osc.state.ny.us/audits/allaudits/093004/03s10.pdf. In order to help ensure that the University has addressed the problems that led to the security breach at issue, we ask you to respond to the following additional questions:

1. According to Mr. Schaffer's report, the disclosure of the student financial aid records was caused by a failure to adhere to "established policies on protecting sensitive and confidential content." In particular, "the University Controller's Office created the Law School directory and did not inform CIS of its existence or request security to be enabled." Under Preventative Action #1 the University indicates that a security policy has been implemented "severely limiting potential exposure and preventing search engines access." Preventive Action #3 indicates that "internal portal content policies" now require a "one-to-one mapping of the security policies to the content update scripts," which "forces CIS participation" whenever changes are required for access to specified content.

Inasmuch as the unauthorized disclosure of education records occurred because of a failure to adhere to existing data security policies, please describe specifically how new policies, or changes to existing policies, implemented by the University will ensure that sensitive data from financial aid and other education records are not made available on an open content server. We are particularly interested in knowing about any machine or human controls that have been implemented or modified in response to this event. Please also describe the results of any testing for vulnerabilities the University has undertaken since implementation of these changes.

2. We note that in regard to the disclosure of records of school employees (which are not subject to FERPA) the University concluded that “[w]hen security was enabled on these directories, errors were made in setting the policies for [these schools]. Testing by the Controller’s Office or CIS did not identify these errors.” Please describe the specific changes the University has made with regard to education records, both in setting policies and testing for vulnerabilities, to ensure that appropriate officials are now able to identify machine and human errors made in setting security parameters on sensitive information.

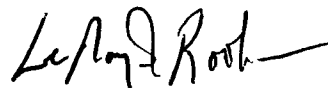
3. The University indicated that the only search engine found to contain the financial aid information was Google, although it is known that both AOL and Yahoo, and possibly others, routinely cache content from websites. Did the University review the preview paragraphs in other search engines to ensure that they did not contain any information from students’ education records?

4. The University reported that the law school report folder was created in August 2005 and that CIS was reviewing its logs to determine how many times this content was accessed. Please advise us of the results of that review, including how many times this content was accessed by IP address sites outside the local area. Have students been advised of the results so that they may take steps to guard against the malicious use of this data?

5. Please describe the University’s response to KPMG’s analysis of any continuing computer system vulnerabilities.

Once again, thank you for you continued cooperation in this matter.

Sincerely,



LeRoy S. Rooker
Director
Family Policy Compliance Office

cc: Dean Marylu Bilek, CUNY Law School
Ms. Angela Joseph, CUNY Law School