Student Files Are Exposed on Web Site

By BRAD STONE

The Princeton Review, the test-preparatory firm, accidentally published the personal data and standardized test scores of tens of thousands of Florida students on its Web site, where they were available for seven weeks.

A flaw in configuring the site allowed anyone to type in a relatively simple Web address and have unfettered access to hundreds of files on the company’s computer network, including educational materials and internal communications.

Another test-preparatory company said it stumbled on the files while doing competitive research. This company provided The New York Times with the Web address of the internal files on the condition that it not be named. The Times informed the Princeton Review of the problem on Monday, and the company promptly shut off access to that portion of its site.

One file on the site contained information on about 34,000 students in the public schools in Sarasota, Fla., where the Princeton Review was hired to build an online tool to help the county measure students’ academic progress. The file included the students’ birthdays and ethnicities, whether they had learning disabilities, whether English was their second language, and their level of performance on the Florida Comprehensive Assessment Test, which is given to students in grades 3 to 11.

Another folder contained dozens of files with names and birth dates for 74,000 students in the school system of Fairfax County, Va., which had hired the Princeton Review to measure and improve student performance.

The Princeton Review said the student information should have been protected by a password, but that the protection was most likely lost when the company moved its site to a new Internet provider in late June. The company said it was looking into how many people might have accessed the files, some of which could be found through search engines.

“As soon as I found out about this security issue we acted immediately to shut down any access to this information,” said Stephen C. Richards, the company’s chief operating officer. “The Princeton Review takes Internet privacy seriously, and we are currently conducting a review of all of our procedures.”

Several other companies have recently committed similar Internet blunders. The British mobile operator O2 misconfigured its cellphone photo service so that its customer’s private images were accessible to anyone using Google. And Facebook recently exposed the birth dates of some users who had wanted to keep them private.

Natalie Roca, executive director for research and testing at the Sarasota County public schools, said she was
“surprised and troubled” by the release of the student data. She said the student information the county gave to the Princeton Review to build the testing tool was strictly confidential.

In addition to the information on students, the site contained the Princeton Review’s educational materials for the LSAT, PSAT and SAT exams, course schedules, an internal analysis of the effectiveness of the company’s instructors, and the entire texts of some Princeton Review books, like the 2008 edition of “Cracking the LSAT.”

One folder on the Web site gave unusual insight into how test preparation companies use older exams to prepare their practice tests. The folder contained digital scans of eight official SATs and six PSAT exams from 2005 through 2007. The tests are created by the Educational Testing Service, a nonprofit organization in Princeton, N.J.

An accompanying guide for Princeton Review exam writers, dated January 2008, said that the company’s “current SAT course diagnostic tests are not as reflective of the real E.T.S. tests as they should be.” It then described “spiraling,” or writing a new practice question based on an old question from the official test. The document instructs authors to avoid copyright infringement by obeying the “three word rule” — ensuring that no three consecutive words remain the same.

Ray Nicosia, the executive director of test security for the Educational Testing Service, said the company had retired the exams that were made available on the Princeton Review Web site and now sells them to tutorial companies. He said he would need more information to determine whether the Princeton Review had properly attained and used the exams.

The Web error indicates that the Princeton Review neglected several accepted online security practices.

In addition to failing to properly restrict access to the student information, the company combined confidential and innocuous files on the same computers — which security researchers say is never a good idea.

“In this case it would have made sense for the company to separate information such as the names of the students from their test scores and whatever confidential information the company had,” said Mike Haro, an analyst at Sophos, an Internet security firm. “But we are finding that companies today don’t change until they have experienced the pain of a data breach that is exposed to the public.”