ACLU
AMERICAN CIVIL LIBERTIES UNION
of OHIO
FOUNDATION

October 17, 2005

Gregory Seibert, Director
Office of Security & Compliance
Kent State University
PO Box 5190
Kent, Ohio 44242

SENT VIA U.S. MAIL & VIA FAX TO: 330/672-9374

AMERICAN CIVIL
LIBERTIES UNION
OF OHIO FOUNDATION
4506 CHESTER AVENUE
CLEVELAND, OH 44103-3621
T/216.472.2220
F/216.472.2210
WWW.ACLUOHIO.ORG
contact@acluohio.org
a member of
COMMUNITY
SHARES

RE: Use of Social Security Numbers as primary identifiers for student and faculty

Dear Mr. Seibert:

I write you because two recent and much-publicized thefts of computer equipment owned by Kent State University have raised serious concerns about Kent State University's use of Social Security Numbers as the primary means of identifying and tracking students and faculty.

The first incident took place on June 14, 2005 when it was reported a KSU human resources employee had a university laptop computer stolen from his car while in Cleveland Heights. According to press reports, personal information, including Social Security Numbers, for approximately 1,400 staffers was contained on the laptop.

The second incident occurred in August 2005 when four computers and six monitors were reportedly stolen from two deans' offices on the KSU campus. It is believed the personal information of at least 100,000 former and current students, faculty and staff was contained on those computers.

As well, there was a third incident reported in February 2002 whereby a University of Akron student was able to access student and employee information, including Social Security Numbers, because of a technical glitch in the KSU website. It appears that glitch may have went undiscovered but for the admission by the hacker to the University about his efforts.

A recent visit by one of our staffers to your main campus demonstrated several other ways that the dissemination and display of Social Security Numbers was treated in a cavalier way. Included was the ability of hundreds of, if not a couple of thousand, faculty members and employees to easily access the Social Security Numbers of students and faculty by using KSU's internal computer network system typically used for such matters as enrollment and class scheduling. In addition, time cards of student employees were displayed in plain view with those students Social Security Numbers displayed at the tops of the cards. These are but two examples of what I fear are many more. Indeed, KSU's website reveals the University uses student Social Security Numbers for a minimum of eighteen different purposes.

Among universities in Ohio, Kent State University is not alone in having personally identifiable information compromised. In June 2005, a laptop was stolen from an admissions office at Cleveland State University putting the personal information of approximately 44,000 current, former and potential students at risk. Most recently, it's been reported the Social Security Numbers and grades of 21,000+ Miami University students from 2002 were mistakenly made available on the University's website, possibly for as long as three years.

As well, private industry in Ohio has been suffering from the same problem in just this past year. In March 2005, a Lexis-Nexis database was hacked putting the personal information of up to 32,000 people at risk. While over a period of several months in late 2004 and/or early 2005, consumers' credit card information was stolen from a database belonging to Columbus-based DSW Shoe Warehouse.

Certainly, numerous other examples of personal data being compromised and stolen from universities and private companies, both in and outside of Ohio, abound. Indeed, it has become nearly impossible to monitor the news without being made aware of further examples of this type on a daily basis.

The problem of identity theft has become so prevalent that recent surveys suggest at least 7-10 million people are subjected to identity theft every year and the Federal Trade Commission has referred to ID theft as the fastest-growing crime in the United States. This problem is why the American Association of Collegiate Registrars and Admissions Officers recommends that institutions not use Social Security numbers as student identifiers whenever possible. Such concerns have also prompted various universities and colleges in Ohio and throughout the U.S. to severely limit their use of Social Security Numbers for their students, faculty and employees.

After each incident involving Kent State University and compromised data, promises to change the data collection and dissemination practices of the University have been made. The concern of the ACLU of Ohio is that these continually promised changes have not been realized and there appears to have been little visible effort to either make substantive changes or acknowledge that this is a high priority for the University.

It is for that reason that I have enclosed with this letter a formal public records request. The primary purpose of the request is to discern what efforts, if any, Kent State University has made regarding changing its use of Social Security Numbers as a primary identifier of students and faculty.

I look forward to receiving those records and it is our sincere hope that Kent State University will take all necessary steps to ensure that none of its students, faculty or staff become the victims of identity theft because of information obtained or yet-to-be-obtained relating to any of the incidents or practices mentioned above.

Should you have any questions, concerns or comments I invite you to contact me directly at 216/472-2220.

Sincerely,

Jeffrey M. Gamso
Legal Director

cc: Christine Link, Executive Director, ACLU of Ohio Foundation, Inc.
Lloyd Snyder, General Counsel, ACLU of Ohio Foundation, Inc.
Edward Mahon, Vice President – Information Services & CIO, Kent State University
Carol Cartwright, President, Kent State University