THE CALIFORNIA STATE UNIVERSITY
Office of the Chancellor
400 Golden Shore
Long Beach, California 90802-4275
(310) 985-2664

Date: April 22, 1997
To: Presidents
From: Samuel A. Serafici
Interim Senior Director
Human Resources

Subject: SALE OF PERSONAL INFORMATION BY STATE AGENCIES

The Joint Task Force on Personal Information and Privacy of the California State Senate has requested that the Department of Finance assist them in obtaining data from all state agencies including the California State University. The task force will examine a variety of issues that affect individual privacy in the coming millennium. The task force also wants to learn about the sale of personal information by each agency for the past three years (1993-94, 1994-95 and 1995-96). This includes the sale of personal or directory information on both employees and students.

In accord with the discussion in Executive Council on April 22, 1997, I am forwarding a survey requested by the task force to be completed for each fiscal year, if the information sold or cost is different in each of the years. If the information is the same for each year, one survey form is sufficient, but note that the information applies to all three years.

Since the request covers three prior fiscal years, some of the information may no longer be readily available. In such cases, provide as much of the information as is reasonably possible.

Please note that a response from each campus is needed, even if no personal information is sold. Please complete the attached survey by May 1, 1997. The survey should be sent by facsimile directly to Noel Grogan at (562) 985-2070.

If you have any questions regarding the survey, please contact Noel Grogan at (562) 985-2664.

SAS/cd
Attachments

Distribution:
Executive Vice Chancellor Broad
Senior Vice Chancellor Lindahl
Vice Chancellor Patino
Deputy Director Yelverton
Director Jones
Senior Human Resources Consultant Grogan
<table>
<thead>
<tr>
<th>AGENCY/DEPARTMENT NAME</th>
<th>FISCAL YEAR</th>
<th>ALL THREE FISCAL YEARS</th>
</tr>
</thead>
</table>

1. **DOES YOUR AGENCY SELL ANY PERSONAL INFORMATION BY VOLUME SALE TO VENDOR(S)?**
   - [ ] YES  [ ] NO
   - If YES, continue with the survey.
   - If NO, please sign, date, and return this form to Robin Larson of the Joint Task Force on Personal Information and Privacy.

2. **PROVIDE (1) A DESCRIPTION OF THE INFORMATION SOLD, (2) THE AUTHORITY TO SELL SUCH INFORMATION, (3) LIST EACH OF THE PURCHASER(S) OF SUCH INFORMATION, AND (4) IF KNOWN, IDENTIFY THE USE OF THIS INFORMATION BY THE PURCHASER(S).**

3. **DOES THE INITIAL PURCHASER RESELL THIS INFORMATION?**
   - [ ] YES  [ ] NO
   - If YES, cite the authority for the resale.

4. **HOW IS THE INFORMATION DELIVERED TO THE PURCHASER?**
   - [ ] HARD COPY  [ ] TAPE  [ ] DISK  [ ] OTHER (PLEASE SPECIFY)

5A. **WHAT IS THE DIRECT COST TO THE AGENCY TO SELL THIS INFORMATION?**
   - Do not include costs of obtaining this information in the first instance.

5B. **WHAT IS THE AMOUNT OF REVENUE GENERATED FOR THE FISCAL YEAR FROM THE SALE OF PERSONAL INFORMATION?**

5C. **IN WHAT FUND IS THE MONEY DEPOSITED?**

6. **DOES YOUR AGENCY/DEPARTMENT TAKE ANY ACTIONS TO PREVENT THE MISUSE OF THE INFORMATION THAT IS SOLD?**
   - [ ] YES  [ ] NO
   - If YES, please describe the actions taken (include results of audits or other investigations.)

<table>
<thead>
<tr>
<th>SIGNATURE OF OFFICIAL COMPLETING THE SURVEY</th>
<th>PHONE NUMBER</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>PRINT NAME OF OFFICIAL COMPLETING THE SURVEY</th>
<th>DATE COMPLETED</th>
</tr>
</thead>
</table>
Joint Task Force on Personal Information & Privacy

BACKGROUND PAPER

April 1, 1997

The Joint Legislative Task Force on Personal Information and Privacy was established pursuant to SB 1659 (Peace)—Chapter 1025, Statutes of 1996. Senators Peace and Calderon sponsored SB 1659 at their own initiative to spark a thoughtful and collaborative effort to examine a variety of issues that affect individual privacy in the coming millennium.

The basic components and directives of the SB 1659 task force are as follows:

- Summary of mission: make recommendations as to what changes to existing laws may be necessary relative to ensuring that state law adequately protects the right of privacy as guaranteed by Section 1 of Article 1 of the California Constitution and that state law adequately addresses issues raised by the rapidly changing nature of information technology and systems.

- Requires establishment by the task force of an advisory committee comprised of affected industries, public and private organizations and consumer groups.

- Issues addressed by the task force may include (but need not be limited to): direct marketing; practices of the Internet industry; practices of the finance and credit industries; the use and distribution of medical records; the use and distribution of public records; and current mechanisms in place to enforce privacy laws.

- Requires the Legislative Analyst to compile task force findings and recommendations, including any dissenting opinions, into a report on or before March 1, 1998.

The issues involving an individual's right to privacy and all the various practices by private and public entities that challenge that right are age-old. What is unique to those of us living in the 1990s and beyond is the exponential growth of info-technology. The technical ability to amass enormous databases with little or no control over the gathering, use, disbursement and
flow of information is what compels the need for this task force and many other collective
efforts to understand the consequences of the new-world global "infrastructure."

While the challenge of reaching consensus among groups as diverse as the participants to
this process is immense, there is a common goal. The absence of an understanding of and
control over the flow of personal information is disastrous for all. On the side of the
individual's right to privacy, there is a constant danger of identity fraud through hijacking of
electronic (or other) personal information, the proliferation or dissemination of inaccurate
information or the mishandling or improper distribution of information. From a business,
government or organizational perspective, the lack of understanding or proper control over the
infrastructure will certainly result in the eventual implosion of that system whether at the hands
of rebellious consumers and legislators or through technological irresponsibility.

So perhaps the first goal of this task force should be to recognize and declare that some form
of standards and/or legal certainty are for the benefit of all. The subsequent and greater
challenge is, of course, to begin to define those standards and/or elements of the law that will
provide that certainty.

Here are some more specific examples of the philosophical balancing acts a task force such
as this faces:

- **Encryption vs. law enforcement.** Privacy advocates maintain a right for every individual citizen
to enjoy sophisticated encryption technology with respect to any personal information about
them on an electronic superhighway. Law enforcement, on the other hand, maintains that for
public safety and national security purposes, their agencies must have eavesdropping or
encryption code cracking capability to evidence any wrongdoing.

- **Personal autonomy vs. public access.** Government records are allegedly made public to allow
for the free flowing of information in a democratic society. Every individual may have his or
her own personal line in the sand as to when publicizing information about them infringes on a
basic right to privacy. The collection and dissemination of these "cradle to grave" records of
every individual has always been an issue, but the implications are significant given current
database technologies. What is the government's role, for example, in the commercialization of
information it collects and stores?

- **Centralized medical records: costs vs. benefits.** A central medical registry could save an
individual's life if an emergency room doctor in Fargo, North Dakota can access the records of
an individual from Los Angeles, California. But what are the safeguards against such
information getting into the wrong hands for unintended purposes (e.g., denying someone health
insurance or employment).

- **Data matching: the Mother of all Big Brothers.** "Data matching" involves the compilation of
different elements about an individual from two or more sources to form a virtual dossier. A
name and address here, a property tax record there, a record of your annual income over there,
and the result is a fairly complete portfolio about you for sale to the highest bidder.
Disclosure with your cookies? It is possible that every click of your mouse is recorded somewhere so all your interests and behaviors on the Internet can be traced. One can only imagine the marketers eager to get such information. That this happens in the first place may be disconcerting to some. Perhaps the challenge to policy makers is, do we force people to at least inform the mice that they are being followed, or do we allow the mice to “opt out” of being followed and mandate a sort of “cookie monster” to gobble up the crumbs in their path?

This is a mere sampling of some of the questions facing this task force. Other specific issues include workplace privacy issues (e.g., employee monitoring), merchant information gathering, telemarketing, etc. The examples highlighted in this paper are not meant to be exhaustive but to get people thinking about the myriad of areas this Task Force might cover. It is also important to recognize that there is much overlap between issues. One cannot discuss government records without also talking about direct marketing and the information vendor industry.

The proposed Task Force Meeting Schedule outlines a series of topics designed to cover as much material as possible while breaking down the general subject of privacy into manageable pieces. While we may attempt to focus on an issue or two at a time, it should be presumed that the lines are often blurred and that any privacy matter can be freely discussed at any of the meetings.

#  #  #  #  #