UNIVERSITY
OF MIAMI
FACULTY SENATE

Faculty Senate Office
Ashe Administration Building, #325
1252 Memorial Drive
Coral Gables, FL 33146

facsen@miami.edu
web site: www.miami.edu/fs
P: 305-284-3721
F: 305-284-5515

MEMORANDUM

To: Donna E. Shalala, President

From: Richard L. Williamson
Chair, Faculty Senate

Date: April 19, 2013

Subject: Faculty Senate Legislation #2012-33(D) – Report and Recommendations of the Faculty Senate ad hoc Committee on Privacy

****

At its April 17, 2013 meeting, the Faculty Senate unanimously accepted the report of the Faculty Senate ad hoc Committee on Privacy and endorses the recommendations stated within the report. The Senate requested the committee continue its work.

The report and recommendations are enclosed.

This legislation is now forwarded to you for your information.

RW/rh

Enclosure

cc: Thomas LeBlanc, Executive Vice President and Provost
Steve Cawley, Vice President, Information Technology
Charlton Copeland, Chair, ad hoc Committee on Privacy

UNIVERSITY OF MIAMI
SCHOOL of LAW

P.O. Box 248087
Coral Gables, Florida 33124

To:	Faculty Senate, University of Miami
From:	Faculty Senate ad hoc Committee on Privacy
Date:	March 25, 2013
RE:	**Review of Privacy Issues at University of Miami**

The Faculty Senate ad hoc Committee on Privacy: Patricia S. Abril, Associate Professor, School of Business Administration; Charlton C. Copeland, Associate Professor, School of Law; G. Christopher Cosner, Professor, Department. of Mathematics; Stephen J. Schnably, Professor, School of Law.

In the fall of 2013 the ad hoc Privacy Committee (the Committee) was assembled to address the Faculty Senate's concerns about the risks to, and the protection of, privacy at the University of Miami. The Faculty Senate's request did not rise in response to a specific incident, but rather from a general concern about the need to broadly assess the potential risks to privacy at the University. Specifically, the Committee was tasked with the responsibility of assessing risks to privacy, and protocols for protecting privacy, as they related to five areas of concern: (1) On-campus video monitoring; (2) Cane Card Access; (3) Cane Watch; (4) Storage and Access to Faculty Files; and (5) Monitoring and Review of Electronic Communications. Much of the Committee's time has been spent identifying and familiarizing itself with the above-mentioned programs and the University units from which they are administered. The Committee has met with a relevant actor(s) in relationship to each of the specified issues (at least in relation to the Coral Gables campus), and finds this to be an appropriate time to report preliminarily on our findings.

On –Campus Video Monitoring:

The Committee spoke with Vice President for Information Technology and University Chief Information Officer, Steve Cawley, regarding on-campus video monitoring, Cane Card Access and the monitoring of electronic communications. Mr. Cawley reported that there are approximately 625 video cameras in operation on the Coral Gables campus. The cameras are primarily in public places, including parking lots, garages, residence halls, and the wellness facility, among others. From Mr. Cawley's recollection, the first camera was installed in 2009. The installation of video cameras was said to follow "standard operating procedure" with Public Safety. The Committee has not yet spoken with Public Safety to determine the procedure for making and approving of requests to install or requests to review footage. Four areas of concern for further study stand out at present. They are: (1) the absence of a formal policy regarding video footage storage; (2) the absence of a policy regarding non-police use of video camera footage; (3) the

Committee's lack of knowledge regarding the policy that governs the installation of University video cameras; and (4) the absence of a policy regarding the procedures for, and communication of, School-level installation of video monitoring equipment.

The Committee inquired about the storage of video footage collected on the cameras. We were informed that the footage is presently stored for 28 days. However, the storage time is not the result of a formal policy arrived at through a process that includes an evaluation of the security and privacy implications, but rather is based on current storage costs. Mr. Cawley agreed that the inevitable declines in the storage costs could, in the absence of a policy, result in the expansion of the amount of time that video footage is stored. This raised a potential privacy concern to the extent that the allotted time for footage retention did not include an express assessment of security and privacy interests. Given the fact that the usefulness of video footage declines with time, any policy would have to take into account the diminishing security interests over time in establishing a formal policy.

Mr. Cawley was not sure whether there is a formal policy regarding the non-police use of the video footage. The Committee has not yet spoken with University Public Safety administrators. In the event that there is no formal policy, the Committee, at a minimum, is concerned that privacy interests are threatened in cases that do not involve security interests. However, even if a policy were in place, the Committee believes that it might be appropriate to examine the reasonableness of the use of video footage for non-security purposes.

The Committee is unclear about the process by which requests for camera installation is made. Public Safety is responsible for camera installation, and we would like to speak about the process by which requests for camera installation are made and the factors that constitute the decision to approve or deny such a request. Specifically, we are interested in determining whether the decision includes an assessment of the privacy implications at stake in an approval or denial of a particular request.

Finally, during our meetings it came to the Committee's attention that University sub-units have also installed video surveillance equipment. At present the Committee simply does not have sufficient details about these installations to speak with any confidence about them. The Committee is concerned about the role that privacy assessments play in the decision to install such equipment. Also, to the extent that video surveillance equipment is installed in open-access areas (i.e., classrooms), the Committee is concerned about the lack of notice to those whose privacy interests might be implicated through the collection and disclosure of video footage.

Cane Card Access:

The collection of Cane Card Access data raises privacy concerns because the data collected can identify particular persons, and might be used to monitor individual activity. The most common use of the Cane Card Access data is for the collection of information about the overall use (and peak use) of campus facilities (i.e., wellness center, library and dining facilities). As stated above, the Committee spoke with Mr.

Cawley regarding Cane Card Access, and the retention and access to data that might have privacy implications. Mr. Cawley reported that data collected from Cane Cared Access was not used for security purposes. He noted that he could not think of an instance where Cane Card data had been used in a police investigation. He also stated that requests are generally made for deindentified information. Mr. Cawley reported that requests for data beyond data released in ordinary reports were obligated to go through an IT approval process. Requests must be made in writing, and a record of all requests—and the ultimate decision—is retained. Requests were required to include an explanation of the purpose for which the information is sought. The General Counsel's approval is required for the external release any Cane Card Access data. The Committee is concerned about the role that privacy assessment plays in the procedures described above. Recently, the management of Cane Card Access has been transferred from IT to Facilities.

The Committee hopes that the transfer of responsibility of Cane Card Access management from Information Technology (IT) to Facilities will include the transfer of IT protocols and procedures for the release of Cane Card Access information. The Committee did not have the opportunity to speak with Facilties or the General Counsel's office regarding any privacy assessment made in the approval or denial of disclosure requests.

Monitoring and Review of Electronic Communications:

We spoke with Mr. Cawley and Vice President of Human Resources, Nerissa Morris and Director of Audit, Blanca Malagon regarding the University's procedures for monitoring electronic communications. Electronic communications and data include, email messages, text messages, Internet usage activity and computer files transmitted through or stored on University computing facilities, including hard drives and network files and folders. The IT Department has reported that there is no "routine monitoring of electronic communications or other electronic files transmitted through or stored on University computing facilities." Such monitoring and review "may occur only when necessary to protect the integrity of the University computing facilities, to protect rights or property of the University or third parties, or to insure compliance with University policy and applicable law." The IT Department has established protocols that govern the determination of any such monitoring or review.

Prior to every monitoring or review, the General Counsel of the University (or her designee) must provide written authorization. In addition to the General Counsel's approval, the approval of another administrative official is required, depending on the employee subject to monitoring and review. Copies of written authorization for monitoring or review are maintained. The record or results of any monitoring or review of electronic messages are shared on with individuals who authorized the monitoring and review. These individuals may authorize the disclosure of the records or results to other individuals. At the conclusion of the review the individual whose electronic messages or electronic data has been monitored or reviewed must be notified in writing. Copies of the data obtained must be destroyed once they are no longer needed.

Cane Watch:

After conversation with Ms. Morris and Ms. Malagon, the Committee did not uncover independent privacy-related concerns about the Cane Watch program. The University's Hotline Service, which provides an online portal through which anonymous complaints can made to the central administration, raises some concerns because the system administrator is a private entity, Ethics Point. There appears to be a lack of knowledge about the privacy protections or vulnerability of external information data protection. When the Committee met with Vice President and Chief Compliance Officer Rudolph Green, he indicated that he is taking a look at the Cane Watch program to improve its functioning. In general, he said he thought it was important that any process include some attention to privacy issues.

Storage and Access of Faculty Files:

The Committee talked to Director of Faculty Affairs, Bill Tallman regarding the retention of, and access to, faculty personnel files. Faculty files include offer letters, salary letters, pre-tenure reviews, tenure files, among other things. The Provost has review rights of faculty files, otherwise files are not reviewed without the General Counsel's approval. Mr. Tallman reported that there are few requests for review of centralized faculty files. The Tenure Review Board and the Academic Personnel Board, which serves as an advisor to the Provost on tenure decisions, have access to tenure-related information in the file. Though these materials had been hand-delivered in previous years, they are accessible on Blackboard for the first time this year. They will remain on Blackboard until the Trustees vote on academic year 2012-2013 tenure applications, and the information will be removed. The Committee's conversation with Mr. Tallman raised two concerns regarding privacy: (1) the retention of faculty medical records in the Faculty Affairs Office rather than Human Resources, allowing the Provost access to Faculty medical records; and (2) the absence of standardized privacy protocols for decentralized faculty files.

At present faculty medical information is maintained in the Faculty Affairs Office. Mr. Tallman stated that this information is usually submitted in relation to applications for medical leaves of absence, but maintained separately from the faculty files. However, the Provost has access to these files, which poses privacy concerns. Additionally, there appeared to be little central knowledge of the faculty files maintained by sub-units of the University. Further there is no information on protocols to protect the content of such files.

Privacy Officer:

The Committee met most recently with Mr. Green. In that conversation Mr. Green expressed interest in including a "privacy officer" within the organizational structure of the University's new Compliance Office. He also indicated that not all universities with a privacy office have chosen to locate the office within the compliance office. While the

Committee is not ready to make this recommendation, we believe that greater protection of privacy interests within the University be the subject of further study.

Overall Recommendations:

As this reports makes clear, there are areas that this Committee has not yet studied involving the specific issues within our original charge, and we have not had the opportunity to begin to study these issues as they relate to academic units beyond the Coral Gables campus. In light of this, the Committee's recommendation is for additional review of specific issues identified herein, and study of issues beyond the Coral Gables campus. Toward that end, the members of the Committee would recommend continued authorization of its review of privacy issues at the University of Miami for the 2013-2014 academic year.