**Faculty Senate IT Committee**

**April 29, 2005**

DRAFT REPORT TO THE FACULTY SENATE ON THE QUESTION OF FACULTY USE OF E-MAIL

 At its December 3, 2004 meeting, the Faculty Senate passed a motion of the Executive Committee requesting:

 That the IT Committee explore the following issues--What are our rights as faculty regarding the use of the e-mail system on campus? How may faculty use the system to communicate with each other? If information is sent to faculty members via the e-mail system, is this the faculty member’s property, regardless of whether it was sent in an encrypted form?--and come back to the Senate with recommendations.

In the period that has ensued, the IT Committee has taken the following action:

1) In December the chair communicated with Dr. Steven Landry in person and by e-mail with regard to the Senate’s charge.  Dr. Landry directed the committee’s attention to three documents, all available on the Department of Information Technology web page, which summarize University policy with regard to computer use in general and e-mail use in particular.[[1]](file:///C:\\Users\\awadmich\\Desktop\\Old%20Senate%20Files\\archives%20from%20old%20website\\Meeting%20Documents%20and%20Minutes%2004-05\\June%202005\\IT%20Comm%20Email%20Report.htm" \l "_ftn1)  The chair discussed with Dr. Landry the issues involved on several subsequent occasions.

2)  At its December 10th meeting, the IT Committee discussed the issue of e-mail use in detail and identified three specific issues that warranted investigation.  These are:

a) Assess to faculty e-mail databases:  Under what circumstances can a faculty member’s e-mail be monitored or reviewed by another individual or administrative body on campus?   To what extent can the contents of messages faculty members send and receive be considered private information?

b) Confidentiality:  Do faculty members have a right to copy, forward and otherwise disseminate contents of e-mail messages they receive from others?  Is it possible or permissible for any individual to unilaterally label a message “confidential” and to impose sanctions on recipients who fail to comply with this stipulation?

 c)  Sharing of information:  What are the restrictions in place on the sharing of information with groups of recipients?  Can certain lists of recipients be considered “off-limits” for the dissemination of information?  Can a faculty member be held liable for using the “reply to all” function either consciously or inadvertently to send a message to a group that would otherwise not be available?  Assuming that the sending of “broadcast” messages by individual faculty members is impermissible, is there any legitimate forum in which discussions open to the faculty as a whole can take place in an electronic format?

Further discussion of these issues in light of the documents provided by Dr. Landry took place at the IT Committee’s meetings in January and February of 2005.

 3) In late March 2005, two members of the IT Committee met with Deborah Raikes-Colbert, Vice-President for Human Relations, to discuss the questions outlined above.   The committee would like to thank Ms. Raikes-Colbert for her willingness to share her time and knowledge and for her many helpful insights.

 On the basis of these meetings and discussions the committee puts forth the following considerations.  What follows is our attempt to understand as best we could the policies actually in place at the present time as they relate to the questions we have identified as critical.  Specific recommendations will be offered in conclusion.

 1)  Access to e-mail accounts.

 According to the “Guidelines for Appropriate Use of Computing Facilities” authorized users at Seton Hall have a “reasonable expectation” of “privacy from unauthorized monitoring of electronic files and intrusion.”  The document also speaks of the obligation of users to respect “the rights of others to privacy, including the freedom from intimidation, harassment and unwarranted annoyance.” This language, along with our consultations with administrators, lead us to conclude that faculty members under ordinary circumstances have a right to consider the contents of their e-mail databases private and to expect that intrusions will be viewed as a violation of that right.  The university does, however, have certain rights of access, which it can act upon in particular instances.  For example, the university retains the right to make copies of e-mail files for purposes of information security (i. e. back-ups).  The university may also delete files that pose a threat to the community (i. e. viruses) or for purposes of managing resource allocation in accordance with clearly delineated procedures.   In these cases the access is unrelated to the content of the documents.   Examination of the content of e-mail databases can only occur when a specific accusation of misconduct has been made and when the monitoring has been authorized by the appropriate upper administrator – in the case of faculty, by the Provost.  Deborah Raikes-Colbert emphasized that the object of the investigation must be specific and limited: open-ended monitoring of an individual’s e-mail traffic on the basis of a general suspicion or personal vendetta would clearly fall outside the boundaries of the guidelines.  Ordinarily, the faculty member would be notified of an examination of e-mail; however, in certain extreme cases, i.e. immediate threat to life and property, or a subpoena from a government agency, the investigation could take place without the faculty member’s knowledge.

Overall, our findings support the idea that faculty members can and should expect that their e-mail databases will remain private. However, one caveat should be made.  Electronic data can never be completely secure.  While the university takes vigorous measures to protect the security of information stored on its servers, a person with sufficient determination and technical skill may be able to find ways to access that information.   Faculty members may want to bear this fact in mind.  But, although it may be technically possible for the security of our data to be compromised, it is no less of a violation of our rights if and when such an intrusion does occur.

 2)  Confidentiality

 The question of e-mail confidentiality is complex.  The current guidelines do not address the issue directly, perhaps for good reason.  However, on the basis of our consultations, we can suggest some tentative observations.   It would appear that the key factor in issues of e-mail confidentiality is not the medium itself but rather the content of the message and the interpersonal context in which the sharing of the information takes place.

Certain classes of information, such as employment, medical or academic records, are confidential by law and cannot be shared with unauthorized individuals regardless of the medium.   Conversely, there are situations in which information cannot be kept confidential.  A supervisor who receives complaints about the job performance of an employee, for example, is obliged to act on that information.

 Beyond these clearly defined categories there is a great deal of ambiguity.  The “Guidelines for Appropriate Use of Computing Facilities” state that users have a responsibility “to respect the rights of others to privacy, protection of their intellectual property including data, ideas, and copyrighted material, and freedom from intimidation, harassment and unwarranted annoyance.”  These points do not directly address the problem of e-mail confidentiality, but they could be interpreted to suggest three areas in which users may be limited in their right to forward e-mail messages and disseminate their contents:

 a)  Privacy.  Regardless of the medium, sensitive personal information should not be disseminated indiscriminately.   Consider the following scenario:

*Professor A has just been diagnosed with a life-threatening illness.  He confides the diagnosis in an e-mail to Professor B.   Professor B then forwards the e-mail to their entire department with an addendum—“thought this might be of interest.”*

 In this situation one could reasonably conclude that Professor A’s privacy rights had been violated.   But while faculty members may have an expectation of privacy with regard to purely personal information, it is far from clear to what extent these protections apply in work-related situations.   For example:

*Professor C has sent an e-mail to her colleagues criticizing the policies and decisions of Department Chair A.  Professor B thinks the criticisms are unfair and forwards the message to the Chair.   Professor C then files a grievance against Professor B claiming that her privacy rights had been violated.*

Has there been a violation?  The story might continue…

*Department Chair A is outraged by the criticisms of Professor C and sends her a furious response threatening reprisals – a five-day teaching schedule, no summer classes and “Don’t expect a promotion as long as I’m around!”  Professor C forwards the message to the Dean along with a request for protection.  Department Chair A initiates disciplinary proceedings against Professor C claiming violation of privacy rights*.

 While we would not suggest a definitive analysis, it would appear the attempts in both cases to exert privacy rights are questionable at best.  Confidentiality should not be used as a shield to protect individuals from the consequences of bad judgment and inappropriate behavior.  To be sure, individuals may have very good reasons for not wanting their work-related communications circulated beyond their intended recipient.  They may justifiably see such circulation as a violation of personal trust, and would rightly think twice about extending this trust a second time.  However, conflating personal betrayal with violation of University policy is a risky path that could open the door to significant abuse.

 b) Intellectual Property

*Professor B has forwarded to Mr. C a message from Professor A containing unique and original ideas.   Mr. C appropriates these ideas as his own and uses them for his personal financial benefit.*

 Clearly, Mr. C has violated the intellectual property rights of Professor A.  But to what extent is Professor B who forwarded the message liable?   Based on our consultations, we have reason to believe that Professor B could be held liable if he had received explicit notification or could have been reasonable expected to understand that the document was confidential.  If, however, the ideas appropriated had been contained in an ordinary message, then it would be difficult to establish culpability. Merely forwarding a message, in most cases, is not the problem.  It is the act of improper appropriation rather than the transmission of information that constitutes the violation of intellectual property rights.

 c) Harassment

*Professor A sends a message to Professor B.  The next day she finds that her message has been sent to a large group of faculty members with spelling mistakes and grammatical errors highlighted and derogatory comments interspersed throughout. This is only the latest in a string of similar incidents involving not only e-mail, but also verbal encounters.*

 Professor A has clearly been subjected to a pattern of harassment and intimidation and would have every right to expect the University to take measures against Professor B.

The cases above show examples of how the act of forwarding an e-mail message could be construed as a violation of the Guidelines for the Appropriate Use of Computer Facilities.  However the violation arises not from the act of forwarding itself but rather from the content of the messages, the context and the underlying intent.   The medium of e-mail may in fact make it more difficult to create an expectation of confidentiality.  E-mail as a medium is designed to facilitate broad dissemination of information to large groups of people.  Forwarding of e-mail messages is a common and ordinary practice.  To a certain extent, the very act of sending an e-mail message entails a certain relinquishing of privacy, since, practically speaking, it is impossible to control who will ultimately receive it.  Even systems to prevent copying and forwarding can be circumvented.   E-mail users understand these conditions and, under ordinary circumstances, accept the possibility they their messages may be forwarded to other users.  The best way to insure that a message does not circulate is to directly request the recipient not to forward it.  However, as indicated above, we do not feel that users can declare any and all messages officially confidential.  Only messages that fall into a defined category and meet specific criteria of confidentiality should enjoy the protection of university policy.

 3)  Communication to groups of users.

 The document “E-mail Guidelines” posted on the TLTC web site states that “all ‘mass mailings’ also known as broadcasts are processed through the appropriate offices.”  Six offices are then listed ranging from the Office of the President to the Broadcast Account run through IT Services.  The guidelines go on to state that “bypassing the above offices in attempting to send unsolicited emails to large numbers of users is in violation of the above guidelines and will be penalized according to current policies governing employees and students.”

 The difficulty in this policy stems from the ambiguity in the definition of a “broadcast” e-mail.  In a narrow technical sense, a “broadcast” could be understood as a message that is sent out to all members of a particular class of user (determined by the prefix FAC, ADM or STU in the internal address). These are, in fact, the types of messages actually sent by the offices in question, using a specific technical procedure created by IT services.

 In addition to these “broadcasts” in the narrow sense, however, the wording of the policy could be construed to include and any and all messages sent out to large groups of people.  Such messages can be sent by means of the group e-mail lists used extensively by offices and individuals to conduct ordinary business.  Lotus Notes makes it very easy to create and replicate these group lists.  Either by choosing “reply to all” or by copying and pasting the list into the address field, it is possible for any recipient on the list to send a message to the entire group.  Committees and departments often use this feature to facilitate on-line discussion of current issues.  Blackboard has a similar capacity.  One can easily, for example, send a message to the entire faculty of the College of Arts and Sciences by going to the A+S page in the community tab and using the “communications” tool to send a message to all users.

 Attempting to enforce a prohibition on the use of e-mail lists to send messages to large groups of people, we feel, would create confusion and open the door to unfair and inconsistent treatment.  How would one distinguish between groups that are “off-limits” and those that can be legitimately and productively used to facilitate dialogue?  Likewise, it may not be easy to differentiate between innocent or inadvertent messages to large groups and conscious attempts to circumvent university policy.   Restrictions on the use of e-mail lists could be perceived as an attempt to squelch free and unimpeded dialogue within the faculty about issues of concern to the community as a whole.   Given the inherent ambiguity in determining which messages are in violation, faculty members may feel that the policy is being used to punish individuals who have questioned the actions of higher administrators.

 There may, of course, be instances in which there are legitimate reasons for keeping an e-mail group list private.   This can easily be accomplished by placing the list in the “bcc” field rather than the “to” field.  If the party sending the message chooses not to do this, it could be interpreted as tacit recognition that recipients will then have the ability to send their own messages to the group as a whole.

We would note that certain e-mail messages sent to large groups may be in violation of university policy as a result of their content.  For example, students who send commercial solicitations to their classmates using Blackboard would clearly be in violation of the appropriate use guidelines which specifically forbid the use of computers for unauthorized commercial purposes.  Likewise, a message that violated privacy rights or was part of a pattern of harassment could be seen as a breech of policy.   In all these cases, however, the violation arises out of the content of the message rather than the fact that it is sent to a group.

In light of these considerations the committee makes the following recommendations.

 1)  The policy on access to e-mail databases provides an acceptable balance between privacy rights and the legitimate needs of the university.  It should be kept in place and enforced as is.

2) Given the complexity surrounding issues of confidentiality, the committee recommends that the University review policy in this area and consider whether clearer and simpler guidelines could be created.  While we do not recommend any specific measures at this point, we would hope that the guiding impulse should be to maximize the ability to share information and engage in open dialogue while protecting the rights of individuals.

3) The committee recommends that the policy on e-mail use be revised to clarify the meaning of the term “broadcast message.”  The committee feels that the term should refer only to messages sent out to entire categories of users across the Seton Hall community.  Ordinary mailing lists created by offices, departments and individuals should not be included in this definition.

Respectfully submitted,

 Nathaniel Knight

Chair, Faculty Senate IT Committee

[[1]](file:///C:\\Users\\awadmich\\Desktop\\Old%20Senate%20Files\\archives%20from%20old%20website\\Meeting%20Documents%20and%20Minutes%2004-05\\June%202005\\IT%20Comm%20Email%20Report.htm" \l "_ftnref1) The documents are as follows: “Guidelines for the Appropriate Use of Computer Facilities,” <<http://technology.shu.edu/page/Appropriate+Use!OpenDocument>>; “E-mail guidelines,” <<http://technology.shu.edu/page/E-mail!OpenDocument>>; and “Information Security Plan” <<http://technology.shu.edu/page/Information+Security+Plan!OpenDocument>>.