**Memorandum**

F**rom: Bob Flores, Senate Policy Liaison – for the Executive Committee’s appointed ad hoc drafting committee.**

**To: Academic Senate, for meeting of January 7, 2019**

**Re: Update on Proposal for Policy 3-234 and Rule 3-234A – Building Access and Surveillance Systems**

This proposal was presented on the Notice of Intent Calendar at the Senate meeting of November 2018, and it now returns on the January 2019 Debate Calendar for a vote of approval. At the November meeting and again at the December meeting, Senate members were invited to provide input for improvements in the proposal, members of the Senate Executive Committee have had multiple opportunities to provide input, members of the Institutional Policy Committee have been consulted repeatedly, and other members of the University community have similarly been invited to give input during the intervening months. Extensive input was received, and as a result we have made several significant changes in the text of the proposed Policy 3-234. This memorandum for January 7 explains the changes made since November. The contents of the proposal as of November were described in the memorandum presented at the November meeting, and a copy of that earlier memorandum is attached below for your convenience.

The Senate is now asked to approve the contents of the proposed Policy 3-234, and the accompanying proposed Rule 3-234, both of which are included in the agenda materials for this proposal.

All of the text changes in the draft Policy made since the version presented at the November meeting are clearly marked with redline/ underline font markings, those parts which will be of particular interest are marked with highlighting, and margin comments are included to explain some of those most significant changes. And for your convenience, here are descriptions of the more significant changes.

1. Expanding the permissible uses of surveillance data—beyond criminal activity.

The most important changes are to follow through on a set of issues that were mentioned in the earlier draft, and were described and discussed at the Senate meetings in November and December. They involve balancing of concerns for individual privacy, with concerns for providing a campus environment that is safe for members of the University community, protecting University resources, and complying with various regulatory requirements. In the earlier draft it was stated that data gathered from surveillance systems would primarily be usable only to detect and deter *criminal* activity. The extensive input we received strongly recommended that the permissible uses be expanded to include situations where there might not be activity that would be technically defined by state or federal law as *crimes*--- but which nevertheless would be of great concern for members of the University community.

In response, we revised the draft Policy to include a list of other situations, not involving criminal activity, for which use of surveillance data could potentially be authorized. However, those other types uses are not freely permitted—each other type of use will only be allowed if explicitly approved in advance through an authorization process which requires approval by the newly established Surveillance Systems Administrators Committee (with representatives of the faculty, students, and staff, as well as administrative officers). And each such authorization of uses for situations not limited to criminal activity must be periodically reported to the Senate.

That newly added list of potentially permissible uses includes:

* An administrative investigation of a potential violation of a *non-criminal law or external regulation* which is directly applicable to the University or University personnel, if such a violation presents a substantial risk of serious harm to the University or any individual (e.g., federal or state regulations regarding storage of controlled substances, or hazardous materials).
* An administrative investigation of a potential violation of a *University Regulation* involving a type and degree of non-criminal misconduct which presents a substantial risk of serious harm to the University or an individual (e.g., posting racially derogatory materials in a University work- or learning-space to create a hostile work/ learning environment for University employees or students; or operating or storing a wheeled riding device in a dangerous manner or in a prohibited zone).
* An administrative investigation by a student-services office regarding a potential disappearance of a campus-resident student, in circumstances in which the student may be at risk of serious harm (e.g., a student housing administrator investigating concerns of a minor student’s family about the student’s well-being after a long period without contact).
* A practice of routinely monitoring the presence of University employees or other individuals in specific locations of a facility of the University Hospitals and Clinics, for the limited purposes of protecting patient safety and ensuring compliance with applicable safety regulations.
* A practice of routinely monitoring the presence of University employees or other individuals in specific locations of a University facility with restricted access, in circumstances in which such monitoring is necessary to comply with directly applicable external laws and regulations or University Regulations such as for protection of sensitive data or regulated technology, or control of special materials (e.g., University Policy 4-004 Information Security; Policy 7-007 Export Control Compliance; Policy 3-300 University Health and Safety).
1. Allowing use of facial recognition software in limited circumstances.

The earlier draft categorically prohibited the use of facial recognition software to track an individual on campus. The revised draft will allow such technology to be used but only in a very limited set of circumstances: “The University will not use facial recognition computer software or equivalent information technology to process video surveillance data to track the presence at a campus location of a particular person for any purpose **other than addressing criminal activity which presents a substantial risk of serious harm to the University or an individual (e.g., a credible threat of a terrorist attack by an identifiable individual at a high-population event on campus).**”

1. Changes regarding retention periods for surveillance data.

The earlier draft included a specified period of time to retain certain types of surveillance data (before automatically deleting the data). We realized such a fine level of detail is inappropriate to include in the main Policy—and should instead be left to be developed by the new SSAC—oversight committee. So that detail is deleted from the revised draft, and instead the SSAC is assigned the task of developing appropriate procedures with specified retention periods for various types of surveillance data.

1. Allowing surveillance systems to be operated by non-University employees—in limited circumstances.

The earlier draft stated that only University employees could be allowed to operate surveillance systems. We received input from the Hospitals and Clinics explaining that in a few instances the University contracts with vendors to operate surveillance systems, at locations of clinics away from the University main campus. The new draft is revised to allow for such contractor-operated systems at off-site locations---but requires that each such contractor-operated system be registered with and approved by the SSAC, to ensure that those contractor-operated systems are operated in accord with the same general privacy-protective principles that apply to systems which are operated by University employees.

--end—

*[See October 2018 memo attached for reader convenience]*

**Memorandum**

F**rom: Bob Flores, Senate Policy Liaison – for the Executive Committee’s appointed ad hoc drafting committee.**

**To: Academic Senate**

**Re: Updated Proposal for Policy 3-234 and Rule 3-234A – Building Access and Surveillance Systems**

**Date: October 30, 2018 [for the November Senate meeting]**

1. Overview:

This is a proposal to retitle and replace existing contents of Policy 3-234 Key Policy with a combination of revised Policy 3-234 Building Access and Surveillance, and new Rule 3-234A Building Access and Surveillance.

Recent developments—input from the Executive Committee and an ad hoc drafting committee.

The proposal project has been underway since early 2018. A version which had been approved through the usual policy development process, including approval at the vice-presidential level, was presented to the Senate Executive Committee September 17. EC members identified numerous concerns about the protections of privacy in the proposal, and the EC determined that it would need substantial further review and likely revision before being brought to the Senate for formal approval. The EC appointed two EC faculty members with expertise in privacy law (Randy Dryer--Law, Leslie Francis—Law) to join with the Senate Officers and work with the existing drafting committee members, to serve as an ad hoc drafting committee, to address the concerns and develop a revised proposal ready for presentation to the Senate. At the October Senate meeting an overview of the project was presented and members were invited to provide input (and from that student representative Devon Cantwell was added to the ad hoc committee). Further discussion took place at the October 15 EC meeting. Numerous drafts have been produced and reviewed within the ad hoc committee, leading up to the proposal now being submitted for the November 5 Senate meeting on the “Intent Calendar.”

The proposal now presented includes (i) explanatory memo; (ii) Policy 3-234 draft, (iii) Rule 3-234A draft, and (iv) an example of a University Procedure 3-234 (providing an example of a formal Procedure which would be approved and implemented by the “SSAC” committee which is proposed to be created).

**On request of the EC, the Policy includes a specific provision requiring that the new regulatory system and contents of the Regulations be reviewed in year 2020 and a report with recommendations be presented to the Academic Senate by October 2020. This will ensure an opportunity for revising of the Regulations as may be needed based on experience over a startup period. The Policy will also require ongoing annual reporting to the Senate, and provides a mechanism for any person concerned about operation of a surveillance system to bring a concern about privacy to the Senate President and in turn to the Senate Executive Committee, at any time.**

**And it is clarified that this current Policy and Rule are focused on primarily *fixed-location* surveillance systems—permanently associated with a particular space. There will subsequently be developed other regulations provisions to address primarily *mobile* systems, such as drone cameras or body-worn cameras.**

1. Background.

The proposed set of Policy and Rule will replace the previous Policy 3-234 Key Policy. That existing Policy’s content was developed at a time when the technology for controlling access to buildings and interior spaces consisted only of mechanical locks and physical keys, and when there was no widespread usage of video cameras or other surveillance systems. That content had not been updated in more than 20 years. In these past two decades, building access and campus security technologies and practices have evolved to include electronic door locks and pervasive camera surveillance systems. The existing 3-234 is completely inadequate to address issues arising with the newer technology, and other regulations do not adequately address the multitude of important issues. The modern rapidly spreading use of electronic door controls and surveillance systems which collect images and other electronic data is raising privacy concerns—which should be but until now have not been addressed in regulations.

The proposal is to update the contents of our regulations to reflect the current extensive and anticipated even more extensive usage of the modern technologies—through a regulatory system that will recognize and appropriately balance issues of privacy, and of campus safety and security. The archaic existing Policy contents would be replaced with a combination of a greatly revised Policy, one associated Rule for now (and likely other Rules to come later), and authorize a new committee to promulgate additional guidance documents with further details.

1. Highlights of the revised Policy
* A comprehensive regulatory system will be established, regulating most of the building access systems and video surveillance systems which are operated by the University on the main Salt Lake campus, and at other satellite campus areas controlled by the University.
* The new Surveillance Security Administrators Committee will be created to serve as the primary oversight body for that regulatory system. It will be assigned broad responsibilities to establish and implement oversight procedures. The SSAC will be comprised of administration representatives (including Public Safety, Office of General Counsel, and Facilities Management). And as specifically requested by the EC, it will include two representatives of the faculty (selected by the Senate Personnel & Elections Committee), and representatives of staff and students.
* As the most important long term component--- all existing building access and surveillance systems, and any new systems, will be required to be registered with and approved through the regulatory system overseen by the SSAC, and will then be periodically reviewed for re-approval. The SSAC will develop and implement a reasonable timeline for the registration process, and a comprehensive set of review criteria which must be consistent with certain fundamental principles already specified in the proposed Regulations.
* Exemptions from the registration & approval requirement will be grantable for some types of small-scale access & surveillance systems which are not appropriate for the University-wide regulatory system.
* The regulatory system will recognize differences between the centrally-operated systems which typically are installed in more open public areas, and smaller systems installed in specific buildings or smaller sections of buildings and operated locally by specific departments. Both types will be regulated under generally similar criteria, but with variations as appropriate for the various types of systems.
* Once the registration and regulatory system is implemented, collecting of surveillance data will only be allowed by systems which have been registered and approved (unless specifically exempted).
* The SSAC will develop and implement a set of criteria for the training, qualifications, and regular oversight of system operations personnel, and only such qualified personnel will be allowed to operate systems and thereby have routine maintenance access to stored surveillance data.
* The storage of surveillance data will be very highly restricted—retention periods will be imposed by the SSAC, and data storage systems must meet security criteria and other design criteria established by the SSAC.
* The regulatory system will balance concerns of safety and security and concerns of privacy. The placement of surveillance systems and the uses of surveillance data by University offices & personnel will be very highly restricted. In general, the University will only use surveillance data for furthering campus safety and security—deterring and detecting criminal activity, to protect members of the University community and lawful visitors, and prevent property theft or damage.
* In particular, there will be *restrictions on*: collecting of audio surveillance date with discernable human voices (i.e., no monitoring of contents of conversations); use of facial recognition software to track persons; and video surveillance of essentially private spaces such as faculty & staff individual offices, bathrooms, etc.
* Some limited exceptions to the above tight restrictions on use will be possible only with specific advance approval of the SSAC and the Office of General Counsel.
* Without exception—the University will not use surveillance data to monitor a student’s course attendance or an employee’s compliance with workplace attendance requirements.
* Regular users of particular spaces should be consulted when systems are being considered for initial installation—e.g., employees and students of a department should be consulted when a system is being considered for the space occupied by that department.
* Appropriate signage must be installed to alert occupants of the presence of surveillance systems.
* Operation of systems and storage and use of surveillance data must be in compliance with various applicable federal laws which address individual privacy and campus safety—including the Family Educational Rights and Privacy Act (FERPA) regarding student records, the CLERY Act regarding campus safety and security, the Health Insurance Portability and Accountability Act (HIPAA) regarding health care patient information
* It is recognized that under the Utah Governmental Records Access and Management Act (GRAMA), the University is defined as a governmental entity, and University records, including stored surveillance data, are governmental records, which may be subject to public records requests. The Policy recognizes that the University must comply with GRAMA when records requests are made—but affirms that the University will protect individual privacy to the fullest extent possible under the applicable law in such cases.
* Academic researchers, including University personnel conducting academic research, may request access to stored surveillance data—and such requests will be processed under the terms of GRAMA—in which case the Policy affirms that the University will also protect individual privacy to the fullest extent possible under the applicable law. Research in such cases would also be subject to typical requirements for research involving human subjects—such as review by the Institutional Review Board.
1. Highlights of the new Rule.
* The Rule addresses managerial issues for building access and surveillance systems, including the methods for funding of initial installation and then ongoing maintenance, and the responsibilities for operations.
* For legacy technology of manually operated mechanical locks and keys, the Rule provides for methods of issuing regular keys and master keys, allocating costs for keys, and processes for re-keying necessitated by loss of control over keys.
* In accord with a provision in the main Policy allowing for exemption of some types of surveillance systems from the ordinary registration and approval process—the Rule specifies certain types of systems/ uses which will typically be exempted (as will be further described by the SSAC).
1. The Example of an SSAC-developed *University Procedure*.

This document is included in the proposal as means of showing Senate members how the SSAC is likely to proceed with implementing the new regulatory process. It describes a potential approach to setting a timeline for surveillance systems to be registered—possibly on a staggered schedule. It has an example of a checklist such as the SSAC will develop and use for reviewing and approving surveillance systems which are to be registered.

1. Consultation and Approvals.

Prior to the presentation to the Senate Executive Committee and the appointment by the EC of an ad hoc committee which then substantially revised the proposal, the proposal had been developed over most of year 2018 by a team including Police Chief Dale Brophy, Facilities Management Executive Director Cory Higgins, and Senate Policy Liaison Bob Flores. It had been reviewed through the Institutional Policy Committee (on multiple occasions), the Office of General Counsel, and the President’s Executive Leadership Team. It had been approved by Vice President for Administrative Services John Nixon.

It has subsequently been very substantially revised with involvement of the EC appointed ad hoc committee. Subsequent to Senate approval, it will ultimately be presented for final approval of the University President and the Board of Trustees.

It is proposed that the revised/new regulations take effect immediately upon final approval.

Questions about the proposal may be addressed to:

Bob Flores, Senate Policy Liaison robert.flores@law.utah.edu

Cory Higgins, c/o Executive Assistant Karen Janicki, Facilities Management

(801) 581-7389 karen.janicki@fm.utah.edu