Safety and Security Video Surveillance--WSU Pullman

PURPOSE

The purpose of this policy is to regulate and standardize the use of all electronic video surveillance systems at the Washington State University (WSU) Pullman campus. The policy also formalizes the installation, management, security, access, monitoring, retention, dissemination, and destruction procedures associated with such systems in order to meet technical and privacy best practices.

POLICY

The WSU Office of Public Safety, with support from Finance and Administrative Information Services (FAIS), is exclusively authorized to select, coordinate, operate, manage, and monitor all video surveillance systems pursuant to this policy.

This policy authorizes a Video Surveillance Oversight Committee (VSOC) established by the Vice President for Finance and Administration to oversee its execution and review. (See Video Surveillance Oversight Committee (VSOC).)

Scope

This policy applies to the use of the video surveillance systems of the Washington State University Pullman campus, and to all personnel, departments, units, and colleges of the Pullman campus. (See Video Surveillance System for a definition.)

Exception

This policy does not apply to video equipment or content produced and used for:

- Institutional Review Board (IRB) or Institutional Animal Care and Use Committee (IACUC) approved research with human subjects or animals;
- Classroom capture;
- Creative or artistic purposes;
- Video conferencing; or
- Police body cameras.

Permitted Uses and Placement

A video surveillance system may be used actively or passively primarily for:

- Enhancement of personal safety;
- Enhancement of property protection;
- Surveillance of criminal or suspected criminal activity;
- Substantiation of civil complaints.
Safety and Security Video Surveillance--WSU Pullman

Cameras

Cameras should only be used in public areas where there is no reasonable expectation of privacy.

Public area camera applications where the camera view includes the outside of any residential facility or private offices must not:

- Offer an enhancement of view of private areas that is better than what is available with unaided vision; and
- Violate a reasonable expectation of privacy.

Signage

Signage is not required for video surveillance installations in public areas. Requested signage must be approved by the VSOC and paid for by the requesting department.

Complaints

Complaints concerning the placement or use of the video surveillance systems should be made to the chair of the VSOC for investigation and adjudication by the committee.

An appeal may be addressed to the Vice President for Finance and Administration within 30 days after the VSOC issues a decision regarding the specific complaint.

Prohibited Uses

Video surveillance equipment uses are limited to professional, ethical, and legal uses that do not violate a reasonable expectation of privacy.

A video surveillance system may not be used:

- To harass, intimidate, or discriminate against any individual or group, including protected groups
- For prurient, immoral, or entertainment purposes, or to view intimate activity
- To record sound or speech in violation of RCW (Revised Code of Washington) 9.73.030, with or without video
- For inoperative or placebo "for looks only" applications unless approved by the VSOC.
Safety and Security Video Surveillance--WSU Pullman

Video Surveillance Oversight Committee (VSOC)

The Video Surveillance Oversight Committee monitors the execution of this policy (*BPPM 50.35*) at the direction of the Vice President of Finance and Administration (VPFA). The VSOC is comprised of representation appointed by the VPFA from campus organizations, which may include:

- Office of Public Safety
- Finance and Administrative Information Services (FAIS)
- Attorney General's Office
- Facilities Services
- Student Affairs
- Office of the Provost

The Vice President for Finance and Administration may select additional members from other campus organizations to serve on the VSOC. Meetings occur at least annually and as needed.

Confidentiality

Personnel are prohibited from disseminating data or information derived from video surveillance systems except pursuant to official and authorized purposes or as required by law. All information and/or observations made through the use of security cameras are considered confidential and may be used for official University and law enforcement purposes only.

Destruction or Tampering

Any person who tampers with or destroys a video surveillance camera or any part of the video surveillance system is subject to appropriate administrative and/or disciplinary action, as well as possible criminal charges.

Content Access, Monitoring, Ownership, And Uses

Video surveillance systems may monitor continuously in real time under normal operating conditions. Typical uses of the system data are for forensic examination.

Access

Access to live or recorded video surveillance data is limited to personnel authorized by the Associate Vice President of Public Safety.

Typically, personnel with administrative or functional responsibilities where video surveillance systems are used are granted authorization to access the data for their specific areas.

Also, all of the following personnel are granted authorization by the Associate Vice President of Public Safety to access the data, unless doing so compromises an investigation:
Safety and Security Video Surveillance--WSU Pullman

Access (cont.)

- Police department personnel
- FAIS personnel
- Public Records Office personnel
- Human Resource Services (HRS) investigative personnel
- Internal Audit investigative personnel
- Senior University administrators (vice president, dean, and above)

Requests for Exceptions

The Associate Vice President of Public Safety may grant exceptions to the access guidelines listed above on a case-by-case basis. Departments must submit a Security Camera System Access Request to the Office of Public Safety to request access for personnel not listed above.

Copying, Duplicating, and/or Retransmission

Copying, duplicating, and/or retransmission of live or recorded video is limited to persons authorized by the Associate Vice President of Public Safety or designee, or as required by state law.

Ownership

All video surveillance system content is owned by the University and is the responsibility of the Associate Vice President of Public Safety under the direction of the Vice President of Finance and Administration.

Uses

Content derived from video surveillance systems may be used in a variety of ways at the discretion of the VSOC and may include non-security uses as deemed appropriate by the VSOC.

Training

All personnel involved in the supervision, application, and use or monitoring of video surveillance systems must be trained with respect to this policy (BPPM 50.35). The Office of Public Safety provides the training.

GENERAL PROCEDURES

Camera Installations

All camera installations must:

- Be completed by FAIS or designee/contractor;
- Comply with applicable building codes; and
- Comply with AMP Netconnect/Commscope Standards.
Safety and Security Video Surveillance--WSU Pullman

Camera Installations Requiring New Cabling

All new camera installations must comply with the requirements and procedures in BPPM 80.56. Facilities Services must complete new cabling pathway/building penetrations for any camera installations, unless such installations are part of a capital project.

FAIS is allowed to install new cabling through existing pathways, as needed, for all new camera installations. All camera side terminations must be completed by FAIS.

Network Activations/ Terminations

ITS is responsible for all network terminations/activations in telecommunications closets.

Storage, Retention, and Access to Recorded Data

Location

All recorded surveillance data must be stored in a secure University centralized location. Individual departments may not store recorded surveillance data except as part of an investigative report.

Contact the Associate Vice President of Public Safety for further information, instructions, and/or authorizations.

Retention Requirements

University records retention requirements apply to video surveillance records.

See the All-University Records Retention Schedule--Security Records table in BPPM 90.01 regarding applicable University records retention requirements for general security monitoring records. NOTE: Retention requirements for police records are covered under a unique departmental records retention schedule assigned to the WSUPD.

Access

Access to stored surveillance data is strictly limited to University employees who have a legitimate business need, as approved by the Associate Vice President of Public Safety.

Access Log

An automatic electronic access log of camera use is created by each surveillance system. The log must include dates and times that cameras are accessed by individuals and the dates and times recordings are reviewed and/or exported.

All logs must be retained for a period of one year as required by federal CJIS (Criminal Justice Information Services) standards and the University's records retention schedule. See the All-University
Safety and Security Video Surveillance--WSU Pullman

Access Log (cont.)
Records Retention Schedule--Information Services Records table in BPPM 90.01.

Release of Information
Persons involved with monitoring, maintenance, or installation must not release any information obtained from University video surveillance systems unless required by law or at the direction of the Vice President for Finance and Administration or designee.

Commercial Use
Commercial use of captured video content must be approved by the President or designee.

Public Records Requests
All public records requests, including requests for the release of video surveillance records, must follow the University's public records request policy. See WAC 504-45-030 and BPPM 90.05.

The Office of Public Safety is responsible for providing any video surveillance records covered by this section (BPPM 50.35) that are requested through the Public Records Office.

DEFINITIONS
The following definitions apply to this section (BPPM 50.35).

Electronic Surveillance
The use of any video device or equipment with the capacity to capture, record, and/or transmit images of places, things, and activities occurring in University-owned or controlled spaces for surveillance purposes.

The cameras communicate with monitors and/or video recorders across private coaxial and/or Ethernet wire cable runs or wireless communication links. For this reason, the cameras are designated as "closed-circuit" to indicate that access to the content is restricted by design only to those able to see it. Modern closed-circuit television (CCTV) displays may include the following features:

• Color, high-resolution displays
• Ability to zoom in on an image
• Ability to track items or individuals

Electronic surveillance subject to this policy (BPPM 50.35) does not include the use of devices or equipment by persons who are not acting within the scope of their authority from the University, or under its direction or control.

Monitoring
The use of cameras, display monitors, or other video equipment for real-time observation of images.
Safety and Security Video Surveillance--WSU Pullman

Permanent Installation
The installation of any device or system that is intended to remain in place for an indefinite time, and to be removed or modified only for change of circumstances, upon approval of the VSOC.

Private Area
An area where an individual might change clothing (e.g., residence, bathroom, shower area, locker and/or changing room).

The term "private area" also typically includes private office spaces. However, exceptions are appropriate in those areas where monetary transactions occur or where the use of CCTV is needed to safeguard money or supplies from theft, destruction, or tampering.

Public Area
An area open for public use where a reasonable expectation of privacy is not violated by what could normally be openly observed (e.g., campus grounds, an academic hallway, a classroom, a library, or a study room).

Surveillance
The use of any device to closely observe any place or thing and to capture, record, and/or document occurrences or conditions for the purpose of securing and protecting the University, its property, and persons in or around University-owned or -controlled spaces.

Surveillance Data
Digital video data captured by recording devices that may be monitored, transmitted, stored, retrieved, or modified in conjunction with the use of an electronic surveillance system.

Surveillance Device
Any camera or video recording device that captures and stores images as data; and any electronic equipment that, as part of a video surveillance system, provides the capability to retrieve, transmit, or reproduce the video data files.

Temporary Installation
The installation of any surveillance device or system that is intended to:

- Remain in place for a defined, temporary period; or
- Remain in place for only as long as required for a specific investigation, trial period, or other short-term need; and
- Be removed when the specified need or period has expired.

Video Surveillance System
A system consisting of electronic devices such as cameras and recording systems designed or used for the purposes of electronic surveillance. The data from the system is transmitted and/or controlled remotely through a direct or network connection.
Safety and Security Video Surveillance--WSU Pullman

REFERENCES

The following references apply to this policy (BPPM 50.35):

- EP15: Policy Prohibiting Discrimination, Sexual Harassment and Sexual Misconduct;
- *RCW 9.73.030*: Intercepting, recording, or divulging private communication – Consent required – Exceptions;
- *WAC 504-45-030*: Availability of public records;
- *BPPM 90.05*: Release of Public Records;
- *BPPM 30.61*: Payment Card Data Security Compliance;
- AMP Netconnect/Commscope Standards.