## Monitoring Online Activities

### Issue Statement:
What information can UC Berkeley collect about the online activities of the campus community for information security protections, what is the acceptable use of this information, and what are the obligations of the campus for the protection of this information?

### Stakes:
Worsening information security threats require a campus response. Increased monitoring will allow for more rapid discovery of more attacks and compromises, and helps align the campus with industry best practice. Industry best practice and increased monitoring comes at a price, as this monitoring may undermine privacy. Privacy is an essential prerequisite for academic freedom, is core to Berkeley's values and human dignity, and a fundamental part of UC Berkeley's reputation world-wide. What is the proper balance between protecting personal (and other sensitive) information held by the Campus and protecting campus members' privacy while on the campus?

### Case for Prioritization:
UC Berkeley is expanding the security program in response to the acknowledged changing threat landscape. All of the proposed enhanced monitoring programs carry the potential privacy risks outlined in "Stakes".

### Input

**Scope:**
Requesting authorization: Information Security and Policy unit under AVC Conrad
Affected: Students, faculty, staff, guests and all users of the campus network, along with all those holding and using CalNet credentials to access resources

**Requested information:**

I. Geographic location of a person using CalNet credentials to authenticate ("geolocation monitoring")
II. Online "fingerprint" of what machines and devices all computers on the UC Berkeley network communicate with ("flow data analysis")
III. Specific unencrypted data leaving the UC Berkeley network ("data loss detection")

**Policy and Practice:**

UC Electronic Communications Policy (ECP) and its campus interpretation
UC Statement of Privacy Values and Principles
CA Data Breach Notification Law and other relevant statutory context

**Key Questions:**

1. ECP Interpretation - May monitoring be instituted for the protection of institutional information, or just for the protection of IT infrastructure?
2. What are allowable uses of collected data, beyond the detection of security incidents and investigation of breaches? (Research, physical safety, etc)
3. What is the acceptable level of info (privacy and security) risk?
   a. internal (misuse by UCB employees)
   b. external (compelled disclosure; security breach of monitoring data)

### IRGC Work (Draft)

**Proposed Principles Responding to Key Questions:**

1. **ECP Interpretation:**
   Information AND infrastructure

2. **Allowable uses of collected data beside info security:**
   Research with appropriate human subject review; Reliable evidence that failure to act would result in significant bodily harm or significant property loss.

3. **Acceptable level of info risk:** (e.g., no privacy risk but higher security risk, moderate privacy risk but lower security risk)
   a. internal Manage via policies and sanctions
   b. external Strong security; time limited storage

**Approval Path Options Include:**

- IRGC member constituencies (VCs, colleagues)
- Council of Deans, Academic Senate, Faculty Specialists
- Data Charter Group, IT Governance Groups

### Output

Justification for designated approval path