Requests to OIT Security for suspected Chegg-related student misconduct incidents

Overview

With more exams being held online in the remote learning environment, OIT Security has received requests from faculty that believe their students leveraged Chegg to share exam questions and answers and participate in academic dishonesty. Faculty are able to obtain access logs from Chegg by the suspected students. Faculty would like OIT Security to correlate this access data with logins to UCI services for which OIT Security has access to authentication logs. Since this is not a pre-approved use of authentication log data, it is required to follow the University electronic communications non-consensual access process to gain approvals before releasing that data.

Process

1. Faculty should request from Chegg as much information as possible about the posts on the Chegg website related to their class's exam questions and answers. The access log usually contains date, time, IP address, and sometimes registered username/email address.
2. Review UCI Privacy's Access to Electronic Communications process.
3. Download the UCI Request for Access Without Consent form listed on the bottom of the page in Step #2.
4. The faculty should fill out this form as completely as possible:
   a. Holder: This is the information to be determined. Leave as N/A and note that students are suspected of academic misconduct. "Title of Holder" should read "Unknown (only IP address known)".
   b. Records: Possible UCInetIDs associated with given IP address at a given time from UCI security logs (specify times).
   c. Access: Check Electronic search. IP address (to be provided) matches to UCInetID using same IP address to authenticate to UCI services, performed by OIT Security under supervision of Josh Drummond, least perusal of contents achieved by not releasing raw logs, only suspected matches of specific IP addresses within a specific time period.
   d. Notification: Ideally students are put on notice at the beginning of class that they are subject to UCI's Academic Integrity Policy. However at the very least, the faculty will notify students and Student Conduct when suspicion is confirmed.
   e. Circumstances Permitting Access: "Substantiated reason" to believe violation of University policy - student misconduct violates academic integrity policies.
   f. Consent: The holder has not been asked to consent because we do not know who the holder is. This process will identify who the owner is.
   g. Authorization: Contact information for faculty making the request.
5. Send the completed form to privacy@uci.edu for initial approval, which they will accept or reject with comments.
6. The request will be sent to Campus Counsel for approval.
7. The request will be sent to the Vice Chancellor Student Affairs for approval.
8. The completed approved form will be sent to OIT Security (security@uci.edu) who can provide the requested information if available.
9. The UCI access logs will be sent to the faculty upon completion of the search.