

Resolution Opposing Ongoing "Coordinated Monitoring" by UC Office of the President
Sponsored by: Rebecca Ora

- WHEREAS** the University of California Office of the President (UCOP), as revealed publicly in January 2016, is currently engaged in ongoing "Coordinated Monitoring" on the all UC Campuses^{1,2}; and
- WHEREAS** this "Coordinated Monitoring" involves the "full packet" interception of all incoming and outgoing data on UC networks; and
- WHEREAS** UCOP's "Coordinated Monitoring" initiative was implemented in a covert fashion, wherein IT staff was instructed to maintain complete confidentiality around aforementioned monitoring;³ and
- WHEREAS** this "Coordinated Monitoring" was initially introduced as a security-assessment technique⁴, but later became an indefinite monitoring endeavor⁵, and
- WHEREAS** the systemwide Cyber Risk Governance Committee (CRGC) designed to oversee "Coordinated Monitoring" activities has only included (and continues to only include) a single member of the systemwide Academic Senate⁶ and no student representation; and
- WHEREAS** the University of California's Electronic Communications Policy (ECP) states that, except under some very limited circumstances, "The University does not examine or disclose electronic communications records without the holder's consent" (Section IV.A), that any such examination or disclosure of data is subject to the "least perusal" standard (Section IV.B.1), and that a University designee shall notify any affected individual of the examination or disclosure of their data, along with the reason(s) for such actions (Section IV.B.3)⁷; and
- WHEREAS** UCOP's "Coordinated Monitoring" activities give it the technical capacity to completely reconstitute the content of electronic communications without holders' consent⁸; and
- WHEREAS** this technical capacity calls into question whether the UCOP's "Coordinated Monitoring" activities are consistent with the University's ECP; and

¹<http://www.ucop.edu/information-technology-services/initiatives/uc-information-security/coordinated-monitoring-and-threat-response.html>

² <http://security.ucop.edu/nava-letter.html>

³ <http://www.dailycal.org/2016/02/02/web-cyber-controversy/>

⁴ <http://universityofcalifornia.edu/press-room/ucop-statement-about-ucla-health-cyberattack>

⁵ <http://www.dailycal.org/2016/02/02/web-cyber-controversy/>

⁶ <http://security.ucop.edu/napolitano-letter.html>

⁷ <http://policy.ucop.edu/doc/7000470/ElectronicCommunications>

⁸ Forum on Cybersecurity and Academic Freedom (see footnotes 3 and 4)

WHEREAS UCOP's "Coordinated Monitoring" activities pose a significant threat to academic freedom⁹, freedom of inquiry, privacy¹⁰, and security¹¹ to all students, faculty, postdoctoral researchers, visiting scholars, staff, and other users of the UC network such as public citizens utilizing electronic resources from the UC libraries; and

WHEREAS data collected and stored by the UCOP's "Coordinated Monitoring" activities are subject to being subpoenaed or requested under the California Public Records Act, thereby calling into question researchers' academic freedom, freedom of inquiry, and privacy¹²; and

WHEREAS University of California IT Staff, including Berkeley Associate Vice Chancellor for IT and CIO Larry Conrad¹³, leadership within the Academic Senate¹⁴, administrators, including UC Berkeley Chancellor Dirks, and faculty throughout the University of California system^{15,16} have all expressed concerns with the content and process of the UCOP's "Coordinated Monitoring" activities; therefore be it

RESOLVED that the University of California Student Association, in solidarity with the many members of UC Faculty, staff and administration, adopt a standing policy in opposition to the University of California Office of the President (UCOP)'s "Coordinated Monitoring" activities as an

⁹ Informal discussion of cybersecurity and surveillance issues (see footnote 7). According to the 2013 Privacy and Information Security Initiative Steering Committee Report to the President (<http://ucop.edu/privacy-initiative/uc-privacy-and-information-security-steering-committee-final-report.pdf>), "Autonomy privacy is an underpinning of academic freedom and is related to concepts such as the First Amendment's freedom of association, anonymity, and the monitoring of behavior... [it] also encompasses records created by the individual such as research data, working drafts of research findings, communications of ideas, and opinions" (pg. 9).

¹⁰ Informal discussion of cybersecurity and surveillance issues (see footnote 7). See the University's Statement of Privacy Values (http://www.ucop.edu/ethics-compliance-audit-services/_files/compliance/uc-privacy-principles.pdf) hosted on UC Berkeley's "Privacy Values" webpage: <https://ethics.berkeley.edu/privacy/values>

¹¹ Informal discussion of cybersecurity and surveillance issues (see footnote 7). By intercepting and collecting all incoming and outgoing data on the UC Berkeley network, UCOP's "Coordinated Monitoring" activities actually *create* a security risk by centralizing sensitive information in a single repository. Furthermore, these data are being backed-up using a cloud-type service with Amazon: an additional third party with its own security risks. Finally, "Coordinated Monitoring" raises concerns that sensitive data (such as data on Human Subjects or communication with political dissidents) are not, in fact, as secure or private as researchers or subjects are led to believe.

¹² UCSA acknowledges that just because data can be requested or subpoenaed does not mean that access will be ultimately be granted. Nonetheless, such requests are moot if data are not collected in the first place. For a concrete example of why this has an impact on researchers' freedom of inquiry, consider the recent case of Professor William Cronon at the University of Wisconsin, Madison (<http://www.newyorker.com/news/news-desk/wisconsin-the-cronon-affair>).

¹³ On February 2, 2016, Associate Vice Chancellor Conrad released the following statement approved by Chancellor Dirks: "We believe that the existing UC Berkeley policy that has been in place for a number of years strikes a good privacy-security policy balance, is robust, and reflects this University's best traditions and values. It is the result of a collaborative campus effort that included both staff and faculty, and like them the Berkeley administration believes that all IT policies and procedures, whether system-wide or local, should be transparent and accountable." (Statement confirmed by Associate Chancellor Nils Gilman.)

¹⁴ <http://www.dailycal.org/2016/02/02/web-cyber-controversy/>

¹⁵ http://senate.universityofcalifornia.edu/documents/Cyber-Risk_Statement_Final_3_Feb_2016.pdf

¹⁶ The Board of the University of California - Santa Barbara Faculty Association wrote a letter to the Chair of the Santa Barbara Division of the Academic Senate on February 3, 2016 criticizing the manner in which "Coordinated Monitoring" had been implemented and requesting more information (see <http://utotherescue.blogspot.com/2016/01/ucop-ordered-spyware-installed-on-uc.html>).

infringement upon the values of shared governance, academic freedom, freedom of inquiry, and privacy; and be it further

RESOLVED that the University of California Student Association requests that UCOP cease its “Coordinated Monitoring” activities, and provide a transparency report including the costs of such activities¹⁷ and how collected data have been used; and be it further

RESOLVED that the University of California Student Association demands the inclusion of student representation on the Cyber Risk Governance Committee on both undergraduate and graduate levels, increase Academic Senate representation on the Cyber Risk Governance Committee, and greatly increase the transparency and oversight around future cybersecurity efforts; and be it further

RESOLVED that the President of UCSA be directed, in a timely manner, to share this resolution with the University of California Office of the President, the Chair of the systemwide Academic Senate, the Vice Chair of the systemwide Academic Senate, the University of California Student Regent, and the University of California Student Regent-designate, and to mention student concerns with privacy in the upcoming March 2016 Regents meeting in the UCSA Presidential address.

¹⁷ See, for example:
<https://bconnected.berkeley.edu/privacy-security/uc-berkeley-bconnected-transparency-report>