

USenate Feedback 6/15/17

SafeConnect

Eric E. Johnson, Associate Professor of Law, submitted these comments about SafeConnect to the University Senate in May, 2017. The response is from Madhavi Marasinghe, UND Chief Information Officer. Marasinghe notes that UND is actively looking at extending and further securing wireless access on campus. Part of the process is to review SafeConnect and evaluate the need for its continued use.

Response (Marasinghe): SafeConnect was implemented in 2009 in the residence halls and apartments to accomplish three main objectives 1) to provide authentication for the wireless network, 2) to deal with the threat and spread of malicious software by requiring connected devices to have basic security protections in place, and 3) to provide the capability to quarantine devices that threaten the safety of the University network or violate University policy. Since that initial implementation, SafeConnect has been expanded to provide authentication to all UND wireless network connections. This was done not only to satisfy security best practices, but primarily in response to a mandate by the Department of Education's Office of Civil Rights which required UND to positively identify all network users. SafeConnect no longer blocks devices without protections in place, but it does provide a valuable service by warning the owner if their device and data are at risk because they don't have antivirus installed or if their device is not configured to receive the latest security updates. It also continues to be used, on a case-by-case basis, to quarantine devices that threaten the safety of the network or violate UND policy.

Comment (Johnson): I suggest UND discontinue subscribing to SafeConnect, which requires the installation on network-users' own personal devices of software that has powerful access privileges and uses those to report back to university IT what is going on on a user's computer, including for instance, what software is running and "the existence or non-existence of file types."
[\(http://impulse.com/news/higher-education/\)](http://impulse.com/news/higher-education/)

Response (Marasinghe): Although SafeConnect does provide the capability to apply custom policies based on the existence or non-existence of file types, registry settings, services, and processes on endpoint devices, this feature is not currently being used. However, the functionality could be enabled in the future to support UND policies. Also, SafeConnect does not currently report all software, only the operating system that is on the device, which is needed to ensure that the device is complying with UND policies.

Comment (Johnson): SafeConnect is unnecessary. It's one of those computer-software technologies that is a solution in search of a problem. By reporting back to the university what software is being used by students, staff, and faculty members, SafeConnect supposedly helps to ensure compliance with a provision of the Higher Education Opportunity Act that was lobbied for by record companies angered by peer-to-peer file sharing on college campuses. But SafeConnect is not necessary to comply with that law. As a legal scholar who teaches and writes in the area of intellectual property, my view is that we ought not go beyond what is legally required, especially when doing so involves an invasion of privacy.

Response (Marasinghe): SafeConnect was not implemented to ensure compliance with the Higher Education Opportunity Act. It was implemented to accomplish the three initial objectives, and expanded to all wireless networks in response to a mandate by the Department of Education's Office of Civil Rights. SafeConnect does not currently report on what software is being used by students, staff or faculty. It does however provide the capability to quarantine a device that is sharing copyrighted material in violation of federal copyright laws and University policy.

Comment (Johnson): My understanding is that last semester, UND IT stopped requiring SafeConnect for access to most campus wifi, but that it is still required in some areas, namely the residential halls. I was unable to find out what led to the pull-back on SafeConnect and whether or not it might be expanded back to its former scope in the future, but it seems like now might be a good time to get rid of it altogether.

Response (Marasinghe): SafeConnect continues to be used for authentication on UND's wireless network throughout campus. The only change has been to warn instead of block users when their device does not have the basic security protections in place.

Comment (Johnson): SafeConnect costs UND money. I don't know how much. But I'd be grateful if the University Senate asked the administration. I believe SafeConnect was originally bought as part of a spate of software purchasing a few years ago, much of which was since criticized, and some of which has been unwound and discontinued.

Response (Marasinghe): SafeConnect costs approximately \$37,000 per year for annual maintenance. However, if SafeConnect was removed, another product would most likely need to be purchased to ensure that all individuals accessing the University wireless network are properly identified and authenticated.

Comment (Johnson): To the extent that visitors to campus must install SafeConnect to access the network, it's an embarrassment, as it makes our campus look like naive consumers when it comes to cybersecurity.

Response (Marasinghe): UND became members of eduroam in late 2015. Eduroam allows the UND community to login without SafeConnect. Eduroam is available across campus except in residence halls. Visitors from other campuses who are members of eduroam are able to utilize eduroam at UND. Those who are not members of eduroam can use the guest portal. The guest portal does not require installation of the SafeConnect policy key.

Comment (Johnson): I also think that we ought to be concerned, as members of a university community, by any technological capability whose makers claim is appropriately "Balancing Network Security with Academic Freedom." (<http://impulse.com/news/higher-education/>) There is no reason to "balance" academic freedom against technological capabilities that are invasive and unnecessary.