February 3, 2022

Dr. Roger J. Ward, EdD, JD, MSL, MPA
Provost, Executive Vice President
University of Maryland, Baltimore
Via email
Cc: Dr. Peter Murray, Dr. Courtney Jones Carney, Dr. Patty Alvarez

Dear Dr. Ward:

The USGA Executive Board is writing to express its opposition to the University of Maryland, Baltimore's intent to ban software applications due to their association with China and Russia, based on superficial assertions of national security concerns. Below, find a more detailed description and rationale behind the various concerns the USGA Executive Board holds.

Summary

On December 6, 2022 the Governor Larry Hogan issued a "cybersecurity directive" directing all state agencies to prohibit the use of Chinese and Russian owned applications, such as Tik Tok, a social media application, on their devices and networks. Tik Tok is owned by a Chinese company, Bitdance, and the United States Federal Government as well as other states have expressed concerns over their access to U.S. citizen's private information.

On January 10, 2023 Dr. Peter Murray, the Senior Vice President for Information Technology and Chief Information Officer for the University of Maryland, Baltimore (UMB) informed the University Student Government Association (USGA), through an email to its President, Joanna Ye, that UMB would be banning certain Chinese and Russian owned applications in line with Governor Hogan's directive.

On January 18th, 2023 the USGA Senate convened and discussed this new prohibition. Senators generally expressed doubts and concerns over the motivations of the prohibition and its disproportionate impact on students. The USGA Executive Committee (the Committee) requested and received a meeting with Dr. Murray and Fred Smith, as well as Dr. Courtney Jones-Carney, on February 1st to discuss these concerns. After this meeting, the Committee believes that the stated reasons for the prohibition are without evidenced merit and do not outweigh the negative implications and consequences of this ban. The USGA Executive Committee therefore **OPPOSES** this prohibition in its current form and requests that the UMB administration provide more information about the specific security concerns underlying this decision and how those concerns are uniquely distinguishable from those posed by apps created by developers in other countries. related to this decision. We urge UMB to consider alternative

solutions to the stated cyber security concerns to avoid disproportionate impacts on students with marginalized identities.

I. The prohibition lacks efficacy in accomplishing its stated goals, raising questions about a rational basis for the policy.

As described in the February 1, 2023 meeting between the USGA Executive Committee and Dr. Peter Murray, the prohibition will be executed through a network wide ban of the now prohibited applications. This means that while on UMB networks one cannot access the applications on their devices at all, or the applications cannot connect once opened. However, this alone does not accomplish the stated goals of the prohibition; namely preventing improper access of sensitive student and university data.

If the premise is accepted that the prohibited applications do in fact improperly collect important data, which the Committee cannot concede without more evidence, a mere network ban will not succeed in stopping the improper collection. First, the mere presence of the application on devices would present the bulk of the security threat, not their access to the network. When an application is downloaded it often "asks" for permission to access certain areas of one's device. This access is not necessarily restricted when the application is open or in use; it often can continue in the "background." Given this, if a prohibited application is operating in the background, even while itself is not connected to the network, it may be able to access or record sensitive data while the device is connected to the UMB network. This would make the prohibition utterly meaningless in comparison to a ban of the application on the devices themselves.

Second, devices connected to the UMB network can bypass the prohibition through a virtual private network (VPN). A VPN, as the name implies, simulates a new encrypted network connection allowing users to both protect their network traffic from data collections and bypass network based blockages, such as the one here.

Thus, even if certain applications pose a risk of acquiring certain private user data, less-restrictive mechanisms likely exist to achieve our mutually desired goal of information security.[1] For example, sending out an email that specifically notifies students of applications that collect private user data, describe specific security threats to student and institutional security, and identify steps we can take to mitigate these risks, would likely alleviate many of the threats identified by Dr. Murray. Dr. Murray stated that invalid duo authentication attempts are made and that students are approving such attempts. We have not received notice of these risks. Simple efforts to remind us of the reason for two-factor authentication and how to respond to

[1] Even permissible government restrictions on speech must be "narrowly tailored" and may not "burden substantially more speech than is necessary to further the government's legitimate interests." *U.S. WeChat Users All. v. Trump*, 488 F. Supp. 3d 912, 927 (N.D. Cal. 2020) (citing Ward v. Rock Against Racism, 491 U.S. 781, 799 (1989)).

unprompted requests for duo-authentication may mitigate the risks described by Dr. Murray. Thus, USGA requests that the administration take less intrusive alternative measures to achieve its goals, rather than overly broad software bans defined by national affiliation, that directly affect our access to communicate with family and friends on the university's wifi network and uniquely impact students residing on campus. We would be happy to work collaboratively with the administration to share our ideas on this.

II. The motivations behind the prohibition are, at minimum, suspect.

The Executive Board acknowledges both that there may be legitimate security concerns over the political leadership of China and that there may be information related to this that is not publicly available, and which may change views on this issue, at this time. However, the USGA Executive Board has doubts as to the motivations behind this prohibition.

In his email to the USGA President, Dr. Murray explained UMB's rationale behind the prohibition like this:

> "We have been put on notice that there are operational and reputational risks to continuing to use products by companies on the state and federal ban lists. These entities and products present an unacceptable level of cybersecurity risk to Federal, State, Local Government, Education institutions, and individual consumers. They are known to engage in cyber-espionage, surveillance of government entities and institutions, and inappropriate collection of sensitive information. TikTok's privacy policy reveals the type of information that is collected by their platform and shared with third parties. The excessive data collected includes: browsing history, location data, file names and types, stored data including text, images, and videos, device ID, device settings, and keystroke patterns. By collecting keystrokes, TikTok can acquire user passwords, passcodes, pins, and communications that include personal information."

A. University communications about the application ban have focused on national affiliations, not specific risks.

The University's communications about banning applications have focused not on specific cyber-security threats, but rather the countries where these applications originate, primarily identifying that the University plans to ban applications from companies based in China. Banning software applications based on affiliation raises red flags that this policy is rooted in discriminatory animus, not valid threats to national security.[2] The University has yet to produce an exhaustive list that specifically identifies the applications it intends to ban and the specific threats posed, further substantiating this shared governance organization's concerns that the proposed action may have discriminatory motivations, raising grave constitutional concerns.[3] Banning software applications the Chinese and Chinese-American student community rely upon in a time when xenophobia and anti-Asian violence are on the rise, prompts concerns about the

---

[2] *See, e.g.*, *U.S. WeChat Users All. v. Trump*, 488 F. Supp. 3d 912 (N.D. Cal. 2020).

[3] *See* Hina Shamsi, Jennifer Stisa Granick, and Daniel Kahn Gillmor, American Civil Liberties Union, *Don't Ban Tik Tok and WeChat* (April 14, 2020) (bans of social platforms represent significant First Amendment concerns).

expressive effect of such policies, in addition to the effects implementing such a ban could have on students with families located in China.

While this organization recognizes the harmful actions taken by government actors in China, those actions should not be conflated with a nation's people. As a public university, we should ensure that our actions against any foreign or domestic actor, are based on specific conduct, not affiliation. However, when we inquired about how the actions of domestic applications such as Facebook and Instagram, are distinguishable from those of applications owned by Chinese companies, such as TikTok or WeChat, we were told that the domestic applications were not owned by "bad companies" reinforcing our concerns about a discriminatory animus. When we pressed further, we were told to read the terms of service of TikTok and WeChat in contrast to domestic owned platforms. However, upon reading and comparing these terms of service our questions were not answered nor our concerns about discriminatory motives, allayed.

Many of us are aware of the "national security concerns" described in the media, but we hesitate to accept a vague, unenumerated security threat, without more, given the atrocities that have been justified by assertions of such vague threats associated with foreign countries. Examples such as *Korematsu v. United States*[4] and *Trump v. Hawaii*[5] should leave us all suspicious of government attempts to cite ill-defined national security concerns as a guise for racism and xenophobia. The reasons the university relies upon "do not prove a reasonable relation between the group characteristics…and the dangers of…[cyber] espionage. The reasons appear, instead, to be largely an accumulation of much of the misinformation, half-truths and insinuations…by people with racial and economic prejudice."[6] Superficial national security concerns in combination with discriminatory rhetoric provide *"strong evidence that impermissible hostility and animus motivated the Government's policy*."[7]

Similarly, Former President Trump's comments about banning Chinese companies were largely based in racial animus,[8] and UMB should not permit or promote discriminatory policies based on a national affiliation. Given the historical misuse of government authority, we maintain a healthy skepticism about associational bans that are not rooted in specific conduct that can be meaningfully distinguished from domestic actors. The rise of white supremacist violence in the United States, along with growing authoritarianism, give us pause about the University's

---

[4] 323 U.S. 214 (1944) *abrogated by Trump v. Hawaii*, 138 S. Ct. 2392 (2018) (justified confining all people with Japanese ancestry in concentration camps based on suspicion of allegiance to a foreign adversary, suggesting that such action was not based on racial animus, but rather valid national security concerns).
[5] 138 S. Ct. 2392 (2018) (state university and mosque challenged ban on immigration from six predominantly Muslim countries suggesting it represented discriminatory animus, but the Court upheld the restrictions citing president's discretionary authority to regulate foreign affairs allows suspension of entry based on national security risks).
[6] *Korematsu v. United States*, 323 U.S. 214, 239 (1944) (Murphy, J., dissenting)
[7] *Trump v. Hawaii*, 201 L. Ed. 2d 775, 138 S. Ct. 2392, 2447 (2018) (Sotomayor, J., dissenting).
[8] *See* Samantha Brown, *TikTok: Time to Expand the Equal Protection Clause*, 62 JURIMETRICS 49 (2021).

willingness to participate in this rhetorical campaign without identifying and communicating a specific risk, and instead suggesting national affiliation itself is acceptable to identify threats posed by applications developed in foreign nations. "By blindly accepting the Government's misguided invitation to sanction a discriminatory policy motivated by animosity toward a disfavored group, all in the name of a superficial claim of national security, the [University] redeploys the same dangerous logic underlying *Korematsu*."[9]

B. The prohibition targets a company owned by an international "rival" for the same behavior domestic companies engage in.

Additionally inexorably linked to this prohibition are the target of the alleged cybersecurity and national security concerns; China and Russia. Both are geopolitical adversaries of the United States, and the Committee recognizes the bad actions of their governments on the global stage. However, the rationale Dr. Murray presented did not adequately connect the prohibition to these behaviors.

As cited above, Dr. Murray states " [The Chinese and Russian applications] . . .engage in cyber-espionage, surveillance of government entities and institutions, and inappropriate collection of sensitive information . . . The excessive data collected includes: browsing history, location data, file names and types, stored data including text, images, and videos, device ID, device settings, and keystroke patterns. By collecting keystrokes, TikTok can acquire user passwords, passcodes, pins, and communications that include personal information." However, despite requests, neither in this email nor in the February 1st meeting was a through line drawn between how these applications' access to this voluntarily provided information leads to "cyber-espionage."

This is further highlighted by the fact that nearly every other social media companies' terms of service discuss nearly the same data collection.[10][10] However, despite these stark similarities, no domestic or "ally" based application is being prohibited. One may wish to argue that the domestic or "ally" based applications do not carry the same security problems as Chinese or Russian applications, however this argument fails based on the swath of negative examples. This includes Meta, a U.S. based social media company, agreeing to pay nearly three quarters of a *billion* dollars to settle a suit that alleged the improperly provided user data to Cambridge Analytica, a U.K. based firm that is accused of interfering in the 2016 U.S. presidential

---

[9] *Trump v. Hawaii*, 138 S. Ct. 2392, 2448 (2018) (Sotomayor, J. dissenting).

[10] *See* Meta Privacy Policy - How Meta collects and uses user data | Privacy Center | Manage your privacy on Facebook, Instagram and Messenger | Facebook Privacy (Showing Meta collects chat messages, mouse movements, and transaction information); *See also* Twitter Privacy Policy (Showing Twitter collects chat messages, I.P Addresses, and generally enough information to infer your identity based on the information we collect" even if one is not signed in); LinkedIn Privacy Policy (Showing LinkedIn collects location data, data on ones salary, Data from one's school or workplace, and "other" undefined data). *But see*; Privacy Policy | TikTok.

election.[1111] The Committee cannot escape the facially apparent double standard that is being placed upon foreign applications.

C. UMB's cyber-security preparedness makes this prohibition functionally moot, and therefore limits cyber-security as a viable motivation.

In the February 1, 2022 meeting the Committee asked how prepared UMB was for cyber-security threats generally. Dr. Murray assured the Committee that UMB was utilizing some of the best tools to protect against cyber security, performs monthly awareness tests amongst the UMB staff and faculty, and blocks approximately five million improper network access attempts each day. The Committee applauds the UMB cyber security for doing a good job day in and day out. However, the demonstrated resilience of the UMB network systems calls into question the need for this prohibition. If UMB is truly as secure as it is claimed to be then these now prohibited applications likely pose limited to no risk to sensitive university and student data. For example, if one of these applications were to key track a user and lift a password for a UMB secured system, would not the cyber-security safeguards in place already prohibit the breach? Given this, the Committee again must question the motivations of the prohibition.

D. Peter Murray provides the likely alternative motivation to legitimate cyber-security concerns.

In his email to the USGA President, Dr. Murray acknowledges that the UMB prohibition of these applications was not a statutory or government mandate; the prohibitions were a *choice* on the part of UMB. Peter Murray further states that, "there are operational and reputational risks," to these applications. Therein lies two justifications, operational and reputational. Above, "operational" concerns have been discussed and doubted. As they are, this justification falls short. This leaves "reputational" risks, which are undefined. However, one could make the educated guess that UMB has a desire to maintain their relationship with both the Governor's office, despite that officer holder recently changing, and other institutions making similar prohibitions. These desires do not intersect with cyber security. Further, these desires trend dangerously close to personal or professional desires to maintain oneself on the popular bandwagon. If true, this would be a gross violation of the student's trust; the prohibition of applications and the potential harming of students for petty personal reputation.

III. The prohibition will have a disproportionate impact on certain students.

In large part this prohibition will impact two student groups: 1. Those who rely on UMB network connections for their internet access and, 2. More narrowly, students of Chinese or Russian origin or descent with family or friends residing within China or Russia or who communicated over the now banned applications. Both groups use several of the now prohibited

[11] Meta will pay $725M to settle Facebook user privacy lawsuit | PBS NewsHour

applications for recreation or vital family communications and this prohibition, as planned, would severely hamper or completely prevent these activities. The Committee views this as an unacceptable situation; no student should be functionally barred from communicating with their family or finding stress relief of their choice while in their studies here at UMB.

When this concern was raised at the February 1st meeting, Dr. Murray stressed that students will still be able to access the prohibited applications on their own wifi networks or through cellular data. The obvious and rational retort offered by the Committee was to raise concerns about students without their own internet access aside from the school and/or with limited data on their phones. Dr. Murray seemed unaware that students, or people generally, could (or would be financially required to) have limited data on their phone plans. This lack of insight is concerning; see further discussion in IV. Regardless, as the prohibition is currently planned, students now and in the future may find themselves without access to important lines of communications; this, again, is unacceptable.

IV. The process in which this decision was made was lacking important student input

As the surprise by common concerns and situations expressed to the committee at the February 1, 2023 meeting imply, there was no true student input into this decision prior to its approval. While the prohibition is not currently implemented, there is little doubt that it will be in fairly short order. In both his email to the USGA President and during the February 1, 2023 meeting, Peter Murray explained how his team was endeavoring to do their due diligence in exploring this issue before finalizing it; the Committee commends this effort. However, the due diligence of student inclusion begins at the start of the decision making process, not in the middle or near the end.

Here, the decision to prohibit these applications was already made. Students' concerns were a secondary consideration, if not lower. As evidenced by Dr. Murray's email to the USGA President on January 24, 2023, the USGA, nor any of its officers were aware that UMB was considering the prohibition of these applications. Only after this decision was virtually made (as implied by Dr. Murray's continuous emphasis that school deans, staff, and faculty were purportedly in unanimous support of the ban) were student concerns solicited. Had UMB involved students sooner, some of the concerns herewith may have been addressed or mitigated.

V. The precedent this measure sets risks encouraging or allowing future ill-conceived prohibitions.

On top of the concerns about making such controversial decisions with improperly timed student input, the decision itself has the potential to set a negative precedent. If UMB can, almost unilaterally, prohibit applications used by students for any number of unclear motivations, where is the line drawn? Where is the due process? Without a firm narrowly tailored written rule, crafted with student input, identifying specific prohibited conduct in such situations, the potential

for a slippery slope is limitless. For example, imagine a future protest wracks Baltimore as it did in 2015. Could the governor ban access to sites linked to their view of "domestic terrorism?" Would UMB block access to expressive activism facilitators, often who are Black run and operated, to protect their "reputation?" Imagine another example: the political right continues to embrace white nationalist sentiments. This leads white students to rally online and in person, making other students uncomfortable. Will UMB ban access to those sites? What about the 1st amendment?

Conclusion

In conclusion, this shared governance organization can't help but notice the fact that the United States education system teaches students from a young age about our country's unique guarantees of freedom, liberty, and autonomy. Those liberties are often demonstrated in contrast to the actions of oppressive foreign governments that withhold information from their people. As students at a public university that is seeking to ban information based on where the software is owned, we struggle to understand how this action does not veer into the realm of authoritarianism. Recent reporting of oppressive foreign regimes focus on the oppressive effects of social media bans in silencing political dissent, and we are concerned that a state university banning foreign social media platforms looks eerily similar to the authoritarian power our education teaches us to be wary of.

Moreover, we remain concerned that such a ban will have a disparate impact on students with families in China and Russia, limiting essential modes of communication that allow students to remain in contact with their families**. Thus, we ask University administration to cease action to ban foreign applications, unless there is a specific enumerated security risk to the University's security posed by specific applications, that cannot be mitigated with less intrusive measures**. Further, if the University plans to take specific action against any entity, we ask that the school undertake a thorough evaluation to assess the impact on our *entire* university community, and identify accommodations to mitigate any disparate risks of harm, particularly those that may affect the most marginalized community members.

We welcome the opportunity to further discuss these concerns and collaboratively identify mechanisms to achieve our shared goals of guaranteeing the safety and security of all members of our community.

Sincerely,

Joanna Ye, USGA President
Courtney Bergan, USGA Vice President
Sam Kebede, USGA Parliamentarian

On behalf of the University of Maryland, University Student Government Association, Executive Board