Open Letter from Former Defense, Intelligence, Homeland Security, and Cyber Officials Calling for National Security Review of Congressional Tech Legislation

April 18, 2022

This is a pivotal moment in modern history. There is a battle brewing between authoritarianism and democracy, and the former is using all the tools at its disposal, including a broad disinformation campaign and the threat of cyber-attacks, to bring about a change in the global order. We must confront these global challenges.

U.S. technology platforms have given the world the chance to see the real story of the Russian military's horrific human rights abuses in Ukraine, including the atrocities committed in Bucha, and the incredible bravery of the Ukrainian people who continue to stand their ground. Social media platforms are filled with messages of support for Ukraine and fundraising campaigns to help Ukrainian refugees.

At the same time, President Putin and his regime have sought to twist facts in order to show Russia as a liberator instead of an aggressor. When reporting and images of the atrocities in Bucha began to circulate, along with evidence and testimony pointing to Russian forces as the perpetrators, the Kremlin was quick to label the claims as "fake news."[1] The Russian government is seeking to alter the information landscape by blocking Russian citizens from receiving content that would show the true facts on the ground – and it has already received buy-in from other like-minded states, such as China, whose social media platform TikTok continues to abide by Moscow's rules of "digital authoritarianism." Indeed, it is telling that among the Kremlin's first actions of the war was blocking U.S. platforms in Russia. Putin knows that U.S. digital platforms can provide Russian citizens valuable views and facts about the war that he tries to distort through lies and disinformation.

U.S. technology platforms have already taken concrete steps to shine a light on Russia's actions to brutalize Ukraine. Through their efforts, the world knows what is truly happening in cities from Mariupol to Kiev, undistorted by manipulation from Moscow. Providing timely and accurate on-the-ground information – and disrupting the scourge of disinformation from Russian state media – is essential for allowing the world (including the Russian people) to see the human toll of Russia's aggression and is increasingly integral to U.S. diplomatic and national security efforts. It is our belief that these efforts will play a part in helping to end this war.

Meanwhile, cybersecurity threats from authoritarian regimes are also on the rise. As President Biden recently announced, the United States is facing an extraordinary threat from Russian cyber-attacks, and the private sector "must accelerate efforts to lock their digital doors."[2] In response to this heightened threat environment, U.S. technology companies have accelerated their partnership with the U.S. government and its allies to improve our collective defense. Both in public and behind the scenes, these companies have rolled out integrated cyber defenses, rapidly fused threat intelligence across products and services, and moved quickly to block malicious actors on their platforms. This partnership has resulted in the detection and disruption of a series of significant security threats from Russia and Belarus.

In the face of these growing threats, U.S. policymakers must not inadvertently hamper the ability of U.S. technology platforms to counter increasing disinformation and cybersecurity risks, particularly as the West continues to rely on the scale and reach of these firms to push back on the Kremlin. But recently proposed congressional legislation would unintentionally curtail the ability of these platforms to target disinformation efforts and safeguard the security of their users in the U.S. and globally. Legislation from

[1] https://twitter.com/RT_com/status/1510639733159956483
[2] https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/

both the House and Senate requiring non-discriminatory access for all "business users" (broadly defined to include foreign rivals) on U.S. digital platforms would provide an open door for foreign adversaries to gain access to the software and hardware of American technology companies. Unfettered access to software and hardware could result in major cyber threats, misinformation, access to data of U.S. persons, and intellectual property theft. Other provisions in this legislation would damage the capability of U.S. technology companies to roll out integrated security tools to adequately screen for nefarious apps and malicious actors, weakening security measures currently embedded in device and platform operating systems. Our national security greatly benefits from the capacity of these platforms to detect and act against these types of risks and, therefore, must not be unintentionally impeded.

We call on the congressional committees with national security jurisdiction – including the Armed Services Committees, Intelligence Committees, and Homeland Security Committees in both the House and Senate – to conduct a review of any legislation that could hinder America's key technology companies in the fight against cyber and national security risks emanating from Russia's and China's growing digital authoritarianism. Such a review would ensure that legislative proposals do not enhance our adversaries' capabilities. It is imperative that the United States avoid the pitfalls of its key allies and partners, such as the European Union (EU), whose Digital Markets Act (DMA) passed without any consideration of national security repercussions – despite repeated concerns from the Biden administration, including over potential cybersecurity risks.[3] There were also bipartisan congressional fears that the DMA would benefit "powerful state-owned and subsidized Chinese and Russian companies," which could have "negative impacts on internet users' privacy, security, and free speech."[4] Even in light of these security concerns, the EU's refusal to undertake a national security assessment led to none of them being addressed. The U.S. government must not make this same mistake.

Russia's invasion of Ukraine marks the start of a new chapter in global history, one in which the ideals of democracy will be put to the test. The United States will need to rely on the power of its technology sector to ensure that the safety of its citizens and the narrative of events continues to be shaped by facts, not by foreign adversaries.

Sincerely,

James R. Clapper
Former Director of National Intelligence

Jane Harman
Former U.S. Representative from California
Former Ranking Member, House Intelligence Committee

Jeh C. Johnson
Former Secretary of Homeland Security[†]

Michael J. Morell
Former Acting Director and Deputy Director, Central Intelligence Agency

Leon E. Panetta
Former Secretary of Defense
Former Director, Central Intelligence Agency

Admiral Michael S. Rogers
Former Commander, U.S. Cyber Command
Former Director, National Security Agency

Frances F. Townsend
Former Assistant to the President for Counterterrorism and Homeland Security

---

[3] https://www.politico.eu/article/us-government-in-bid-to-change-eu-digital-markets-act/

[4] https://www.finance.senate.gov/chairmans-news/finance-committee-leaders-wyden-and-crapo-biden-administration-must-fight-back-against-discriminatory-digital-trade-policies

[†] Secretary Johnson is a partner at the law firm of Paul, Weiss, Rifkind, Wharton & Garrison, LLP which has as clients several U.S. technology firms with an interest in the pending legislation. The views expressed in this letter are Secretary Johnson's personal views.