The Washington Post
Democracy Dies in Darkness

Opinion What worries me most after five years as leader of the NSA

By Paul M. Nakasone

February 14, 2024 at 7:15 a.m. EST

Gen. Paul M. Nakasone was commander of the U.S. Cyber Command, director of the National Security Agency and chief of the Central Security Service until Feb. 2. This column was written in his official capacity while still in office.

Approaching the end of my five-plus years as director of the National Security Agency, I have heard the same question again and again: What's your greatest worry as you conclude decades of service to your nation?

People expect me to name a particular country or challenge threatening the United States — maybe China or Russia, or even criminal hackers targeting our critical infrastructure. I have plenty of worries about each of those. What worries me most, though, isn't an external threat, but the possibility that we are on the verge of making a grave mistake.

I worry that we could make ourselves blind to external threats such as the ones I've named and more if Congress allows a critical intelligence collection authority — Section 702 of the Foreign Intelligence Surveillance Act — to expire in April, or renews it with crippling restrictions. Either move would be a self-inflicted wound that our nation cannot afford.

Let me go back in time to explain. I was at the Pentagon when terrorists crashed Flight 77 into the building on Sept. 11, 2001, killing many of my colleagues at the Department of Defense. As the 9/11 Commission examined how our country could have suffered such a devastating attack, it became clear that our government had been unable to connect the dots between terrorist plotters abroad and terrorist operatives on our soil. We needed to tear down the wall between the FBI and the intelligence community that was blocking access to foreign intelligence information that these agencies had already lawfully collected and stored in government databases, so that we could use it to better protect Americans.

We also needed a sensible way to work with U.S. technology companies whose services were increasingly being exploited by terrorists and other hostile actors abroad to plot against us. Congress provided just that in 2008 with the creation of Section 702.

This law strikes an elegant balance in allowing intelligence collection that targets only non-Americans located abroad while imposing stringent protections for Americans' privacy anywhere in the world. Applying it requires the approval of a federal court as well as oversight by the executive branch and four separate congressional committees — meaning that every branch of government has a say in how we can use it.

Fast-forward to 2018, when I became commander of U.S. Cyber Command and director of the National Security Agency. Congress and the president had just reauthorized Section 702 — and for good reason. It works. Indeed, it has become more important than ever given its contributions to thwarting a wide array of national security threats.

Some examples: Section 702 has disrupted planned terrorist attacks at home and abroad, and contributed to the successful operation that killed al-Qaeda leader Ayman al-Zawahiri in 2022. Information acquired through Section 702 has provided insights into the Chinese origins of a chemical used to synthesize the deadly drug fentanyl and into drug-smuggling techniques. Section 702 has helped uncover gruesome atrocities committed by Russia in Ukraine, including the murder of noncombatants and the forced relocation of children from Russian-occupied Ukraine to the Russian Federation. Section 702 has even resulted in the identification and disruption of hostile foreign actors' attempts to recruit spies in the United States.

Perhaps most strikingly, as the undersecretary of defense for intelligence and security wrote in December: "Today, our warfighters depend on intelligence reporting using collection obtained pursuant to Section 702 to provide critical insights on the battlefield, including the current crises in Europe and the Middle East."

Section 702, in short, is essential and irreplaceable. But it is set to expire in April, unless Congress acts to renew it.

Failure to do so would be a self-inflicted wound of the highest order. At this moment, as the United States faces escalating threats posed by China, Russia, Iran, foreign cartels, sophisticated hackers, WMD proliferators, spies, terrorists and more, allowing Section 702 to expire would be an act of willful self-blinding.

The same is true of sweeping proposals to cripple this important authority, including requiring the executive branch to seek approval from a federal court to conduct U.S. person queries, which involves organizing and utilizing information that the government has already lawfully collected. That would be precisely the opposite of what the 9/11 Commission urged: It would erect a new wall blocking our access to intelligence already legally in the government's holdings that could be used to protect Americans, effectively making it inaccessible to our intelligence professionals. That would be a huge step backward.

Instead, we should take a step forward by reauthorizing Section 702 — and improving it. That means enshrining in statute the extensive reforms the intelligence community has already made to prevent noncompliant queries of 702 databases. We are only human, and mistakes happen, but the key is to learn from our mistakes and be transparent about them so they can't happen again. These are the boldest reforms to Section 702 the executive branch has ever proposed in a reauthorization cycle, and they'll better protect both our security and Americans' privacy.

Serving the public in uniform for more than 37 years has been the honor of a lifetime. As head of Cyber Command and the NSA, I urge Congress to reauthorize Section 702, and to do so without imposing new restrictions on how the government can use the vital information it provides. As I saw all too clearly at the Pentagon that morning on 9/11, American lives are at stake.