

December 11, 2023

The Honorable Mike Johnson  
Speaker of the House of Representatives

The Honorable Steve Scalise  
Majority Leader of the House of Representatives

The Honorable Hakeem Jeffries  
Minority Leader of the House of Representatives

Members of the House of Representatives

Dear Mr. Speaker and Members:

As you well know, our nation is under significant threat today with wars in Europe and the Middle East, a potential conflict with China in the Indo-Pacific, and the deadly flow of fentanyl across our southern border. In these circumstances, we cannot hamstring the U.S. Intelligence Community either by failing to renew Section 702 of the Foreign Intelligence Surveillance Act or by limiting it in ways that would make it difficult for the government to protect Americans. To be clear, Section 702 saves American lives and helps keep Americans safe from international terrorist attacks, foreign cyberattacks, overseas fentanyl suppliers, and other threats to our national security. There's no substitute for it.

It is in this context that we, a bipartisan group of former national security officials that served in Republican and Democratic Administrations and on Capitol Hill, write to urgently warn you of the devastating impacts to national security if Congress passes H.R. 6570, the Protect Liberty and End Warrantless Surveillance Act, as reported by the House Committee on the Judiciary.

We appreciate the serious efforts made by both that Committee and the Permanent Select Committee on Intelligence to evaluate Section 702 and consider what privacy and additional protections are needed. In our view, however, the legislation reported out by the Committee on the Judiciary is seriously flawed and would hurt our government's ability to protect Americans in the current heightened threat environment. We outline some of our concerns below.

Most notably, as written, H.R. 6570 could end the Section 702 program entirely. Section 21(d) of the bill enumerates the exclusive provisions of law allowing electronic surveillance, but – in what presumably is a serious drafting error – it fails to include Section 702. As a result, the bill could prohibit electronic surveillance through Section 702 using the compelled assistance of an electronic communications service provider. Ambiguous or erroneously drafted legislation must not imperil America's safety.

H.R. 6570 contains many other unworkable and dangerous provisions with no basis in the Constitution, statute, or caselaw. Below are just a few examples:

- **The bill grants unprecedented rights to foreigners.** The proposed Section 702(f)(1) would extend to foreign spies and terrorists the same protections proposed to be afforded to Americans just because they might be (or have once been) in the United States. This goes against fundamental principles of decades of surveillance law carefully crafted by both Congress and the courts. Under the proposed provision, if a spy recruiter for the People's Republic of China was known to be inside the United

States, that person could not be the subject of a query under the proposed bill unless he (unlikely) qualified for one of the proposal's limited exceptions. Moreover, by extending this "protection" to foreign targets communicating with one another, but not with any American at all, the bill would drastically limit the government's ability to warn Americans that they are the targets of terrorist threats, malicious cyber activity, or espionage operations. Giving foreigners "query protection" does nothing to help Americans' privacy but will instead endanger Americans.

- **The bill would prohibit queries that have kept our nation safe.** The bill would bar the government from querying the Section 702 database with terms associated with Americans unless it first obtains a court warrant. Even when the government could establish probable cause – circumstances rarely immediately present in the fast-moving worlds of terrorists, spies, and ransomware gangs where the government often has merely a tip -- it would still take days to do so. In short, if the Intelligence Community found out that a terrorist overseas was talking to someone inside the United States, it couldn't search its database to determine whether there is an imminent threat to the United States. This will endanger American lives. Moreover, as written, this warrant requirement would apply not just to the FBI—which is the subject of other specific provisions based on prior controversies—but also to the entire intelligence community. This provision, if adopted, would greatly harm the foreign intelligence mission of the NSA, CIA and NCTC.
- **The bill would seriously undermine cybersecurity efforts.** As written, the warrant "exception" for cybersecurity is dangerously narrow and will make it nearly impossible to protect Americans who are victims of foreign cyberattacks every day, let alone recover ransomware payments. Proposed Section 702(f)(2)(B)(i)(IV) purports to allow queries using a "known cybersecurity threat signature." But it isn't clear what a "known cybersecurity threat signature" even means. In any case, it apparently wouldn't cover using actual names, IP addresses or email addresses of targets of malicious cyberattacks. Cybersecurity professionals know that those terms are precisely what's needed to uncover the type and scope of a foreign cyberattack. The result of adopting this provision is that the government simply won't be able to warn American citizens, businesses, hospitals, critical infrastructure owners, schools, and others of many imminent cyber threats.

As former national security officials, we believe the House cannot responsibly adopt H.R. 6750. By contrast, H.R. 6611, as reported by the Permanent Select Committee on Intelligence, represents a thoughtful alternative approach to Section 702 reforms. Reasonable minds might disagree on the details of the various reforms that might be needed, even as included in the HPSCI bill. But it presents a rigorous approach to the challenges and attempts in a responsible way to balance privacy protections and our nation's safety. Enacting H.R. 6750 will, by contrast, greatly hamstring our government's efforts to protect Americans.

Sincerely,

Keith Alexander  
Former Director, National Security Agency

Chuck Alsup  
Former Assistant Deputy Director of National Intelligence

Stewart Baker  
Former Assistant Secretary for Policy,  
Department of Homeland Security

William Banks  
Former Chairman, American Bar Association Standing  
Committee on Law and National Security

George C. Barnes  
Former Deputy Director, National Security Agency

Jeremy Bash  
Former Chief of Staff, Department of Defense

Timothy Bergreen  
Former Staff Director, House Permanent Select  
Committee on Intelligence

Andrew Borene  
Former Group Chief, National Counterterrorism  
Center

Robert J. Butler  
Former Deputy Assistant Secretary of Defense for  
Space and Cyber Policy

James Clapper  
Former Director of National Intelligence

Gary P. Corn  
Former Staff Judge Advocate, U.S. Cyber Command

John Costello  
Former Chief of Staff of the Office of the National  
Cyber Director

George W. Croner  
Former Principal Litigation Counsel, National  
Security Agency

William P. Crowell  
Former Deputy Director,  
National Security Agency

J. Michael Daniel  
Former Cybersecurity Coordinator, National  
Security Council

Courtney Simmons Elwood  
Former General Counsel, Central Intelligence Agency

Daniel R. Ennis  
Former Director, Threat Operations Center,  
National Security Agency

William Evanina  
Former Director, National Counterintelligence and  
Security Center

Bishop Garrison  
Former Senior Advisor to the Secretary of Defense

Michael Geffroy  
Former General Counsel, Senate Select Committee on  
Intelligence

Glenn S. Gerstell  
Former General Counsel, National Security Agency

Jane Harman  
Former Ranking Member, House Permanent Select  
Committee on Intelligence

Adam S. Hickey  
Former Deputy Assistant Attorney General

Jamil N. Jaffer  
Former Associate Counsel to President George W.  
Bush

Richard H. Ledgett, Jr.  
Former Deputy Director, National Security Agency

Michael A. LeFever  
Former Director of Strategic Operational Planning,  
National Counterterrorism Center

Rachel Carlson Lieber  
Former Deputy General Counsel, Central  
Intelligence Agency

Robert S. Litt  
Former General Counsel, Office of the Director of  
National Intelligence

Letitia Long  
Former Director, National Geospatial-Intelligence Agency

Mike McConnell  
Former Director of National Intelligence

Michael Morell  
Former Deputy Director, Central Intelligence Agency

Michael B. Mukasey  
Former Attorney General of the United States

Leon E. Panetta  
Former Secretary of Defense

James Petrila  
Former Associate General Counsel, Central Intelligence Agency

Elizabeth Rindskopf-Parker  
Former General Counsel, Central Intelligence Agency

Harvey Rishikof  
Former Legal Counsel, Federal Bureau of Investigations

Rod J. Rosenstein  
Former Deputy Attorney General

Norman T. Roule  
Former National Intelligence Manager for Iran, Office of the Director of National Intelligence

Teresa H. Shea  
Former Director of Signals Intelligence, National Security Agency

Bryan Smith  
Former Budget Director, House Permanent Select Committee on Intelligence

Suzanne E. Spaulding  
Former Under Secretary, Department of Homeland Security

Megan H. Stifel  
Former Director of Cyber Policy, US Department of Justice

Jan E. Tighe  
Former Director of Naval Intelligence

Frances Townsend  
Former Counterterrorism and Homeland Security Advisor to President George W. Bush

Joseph L. Votel  
Former Commander, United States Central Command

Thomas Warrick  
Former Department of Homeland Security Deputy Assistant Secretary for Counterterrorism Policy

B. Edwin Wilson  
Former Deputy Assistant Secretary of Defense for Cyber Policy

James A. Winnefeld, Jr.  
Former Vice Chairman, Joint Chiefs of Staff

Julie Myers Wood  
Former Assistant Secretary of Homeland Security for Immigration and Customs Enforcement