THE SAFE ACT RAISES PROFOUND RISKS FOR NATIONAL SECURITY AND PUBLIC SAFETY

The Security and Freedom Enhancement (SAFE) Act of 2024 is not a compromise approach to reauthorizing and reforming FISA Section 702. It includes several measures that, if enacted, would undermine national security and public safety.

- First, it effectively bans U.S. officials from reviewing critical communications lawfully obtained under Section 702. This would hamper the ability of the Executive Branch to identify threats and protect Americans.

- Second, it includes broad restrictions on the acquisition of commercially available information, including frontier AI systems, that will hamper the ability of the Executive Branch to identify and disrupt threats, and would put the United States at a disadvantage compared to our adversaries.

***

SAFE Act restrictions on lawfully collected intelligence under 702 will endanger national security

The SAFE Act effectively bans reviews of vital intelligence that the Executive Branch has already lawfully obtained under Section 702 authorities, including about foreigners who are in the United States who have illegally crossed the border or are spying for malicious foreign governments.

- The bill precludes any U.S. government officer or employee from accessing communications content *lawfully acquired under Section 702 authorities* if the content is associated with a United States person or anyone else *"reasonably believed to be in the United States"* when the underlying communication *or* query took place.

- That would mean that if the FBI learned an individual with connections to a major international terrorist organization had just arrived at JFK airport, the FBI would be unable to look at its lawfully collected holdings to learn more about their intentions.

The bill provides four dangerously narrow exceptions to this general ban:

1) A "court order" exception, wherein the person to whom the query relates must be the subject of an existing court order—under FISA or criminal authorities.

    - This exception reflects a lack of understanding about how these queries work.

    - Queries are typically conducted at the earliest stages of an investigation or intelligence analysis to connect the dots. At this point, the U.S. Government almost

never can obtain a court order—including because it does not possess enough information to meet the legal standards.

- If the person related to the query is the subject of a court order, then by definition, U.S. officials already have a sufficient basis for suspicion and would likely not have a need to query 702 information, in order to determine the national security threat that he or she might pose.

2) An extremely narrow **"**emergency" exception.

   - This is limited to situations involving an "imminent threat or death or serious bodily harm" in which the communications "must" be accessed—employing criteria that will rarely be satisfied.

   - Queries are often run to determine if an emergency exists—but could not be, under this exception.

3) A case-by-case "consent exception," wherein a third party legally authorized to consent on behalf of the subject of the query has done so.

   - When responding to rapidly developing national security threats, there is often not sufficient time to identify, locate, and obtain consent from a private party. The problem is compounded when, as is often the case, threats implicate many individuals.

   - At an early stage of an investigation, it is often not clear whether a person is a victim or perpetrator of malicious activity. In seeking consent, there is a high risk that the government inadvertently tips off a bad actor.

4) A "cybersecurity exception," wherein the communications content is accessed and used for the sole purpose of identifying receipts of malicious software and preventing or mitigating harm.

   - The bill specifies that the Executive Branch can only review "malicious software and cybersecurity threat signatures" to identify victims of and mitigate harm from cyberattacks.

   - It states that "no other communications content or other information" can be accessed or reviewed.

   - This excludes many common means of cyberattacks—such as spear phishing emails, denial of service attacks, or exploiting zero-day vulnerabilities—severely limiting the utility of the exception.

SAFE Act restrictions on commercially available information (CAI) will hinder the U.S. Government's ability to identify and disrupt threats to Americans and the homeland.

Commercially available information (CAI) provides vital insights for the conduct of modern intelligence and law enforcement activity—enabling us to track the global shipment of drugs, execute cyber operations, and understand Russia's war plans. The SAFE Act imposes broad restrictions on the ability of the government to purchase or otherwise acquire critical data that is commercially available.

- The legislation precludes the IC from acquiring a dataset that includes "data, derived data, or any unique identifier" that is reasonably linked to a (i) US person or (ii) a foreigner in the United States, at the time that data was created or acquired. Law enforcement is subject to an even broader ban.

- In practice, these exacting standards will be very difficult—and in some cases impossible —for the IC or law enforcement to meet.

    - As a practical matter, there is often no way to establish even a "reasonable belief" of whether a particular individual was inside the United States at the time a particular piece of data was created.

    - Even if an individual's location at the time data was created could be determined, the plain language of the bill would prevent, for example, the IC from acquiring information regarding foreign government officials who visited the United States as well as foreign spies, terrorists, or drug traffickers who illegally crossed the border and later departed the country.

- The narrow "exceptions," intended to diminish the impact of these restrictions, will rarely apply—and when they do, onerous use and other provisions still will dramatically undercut the government's ability to benefit from CAI.

These restrictions will significantly hinder the government's ability to identify and disrupt threats and put us at a disadvantage compared to our adversaries, who can readily access such data.

- The IC would be barred from acquiring the types of information necessary to detect and defeat adversary cyberattacks—information that is routinely available to commercial sector entities for basic cybersecurity activities.

- The bill would also ban the IC from acquiring information necessary to protect its installations, activities, facilities, and property.

- Most notably, the bill may significantly limit the government's acquisition of essentially all frontier AI systems (e.g. large language models)—limiting our ability to improve our

cyber defenses against increasingly sophisticated exploits, increase the precision of critical weapons systems, and protect our troops.

- Meanwhile, the bill does nothing to stop China, Russia, Iran, other hostile foreign governments, cartels, human traffickers, and other transnational criminal organizations from continuing to purchase and exploit commercial data to steal our intellectual property and harm our citizens, critical infrastructure, and our national security.

We agree that more needs to be done to protect Americans' data privacy. But this bill is not the vehicle for that action.

- Last month, President Biden issued a sweeping, historic executive order to prevent the large-scale transfer of Americans' sensitive personal data to countries of concern. This is the most significant action any President has ever taken to protect American's data security—and underscores the Biden-Harris Administration's abiding commitment to protecting privacy and civil liberties.

- And soon, the Director of National Intelligence will issue binding, IC-wide guidance setting out rules for identifying and handling sensitive CAI, and for mitigating privacy and civil liberties risks associated with it.

- Currently, all IC elements' acquisition and use of CAI must comply with the Fourth Amendment, other applicable legal restrictions, and implementing policies. The DNI's forthcoming guidance will add further protections.

- The IC is committed to working with Congress to further protect Americans' data privacy without unduly harming our national security.