February 20, 2026

Stewart Baker's
Answers to Written Questions from Members of the Senate Judiciary Committee
after a January 28, 2026, Hearing on
"Review and Reform: The Foreign Intelligence Surveillance Act and Executive Accountability"

Answers to Questions from Committee Chairman Charles E. Grassley

1. **Please explain what it means to "query" information lawfully collected pursuant to Section 702 and why requiring a warrant for US person queries would be detrimental to national security.**

Section 702 allows the government to collect the communications of foreign intelligence targets like Hezbollah or the Chinese security services when those targets use U.S. communications systems. The government obtains authority to intercept those communications by following procedures overseen by the Foreign Intelligence Surveillance Court (FISC or FISA Court). The interceptions are fully authorized under U.S. law. The contents of the communications are provided to only four intelligence agencies (the CIA, NSA, NCTC and the FBI), and those agencies store them electronically so that the contents may be queried by intelligence officials.

A "query" in this context is like the search tools we all use when we hit CTRL-F to find particular words in a large document or when we ask Google to find a particular message in our Gmail rather than looking through each email individually. Such tools allow us either to quickly determine that there is no relevant data in the database or to determine where the relevant data is. It's a fast, efficient way to retrieve information we already have.

That's how the government uses section 702 queries. And that's why requiring a warrant for queries is such a bad idea. First, it imposes lengthy delays and roadblocks on a process that today can be accomplished in seconds with a few keystrokes. When the government is trying to find out whether a foreign terrorist or spy has recruited an American, delay can be fatal. Second, a warrant is an unprecedented requirement for government queries of data that the government has already lawfully collected. For data that is already lawfully stored in a government file cabinet, no one has ever said that investigators can't open the cabinet without a warrant, even if they are looking at a new suspect.

Those who want to require warrants for 702's filing cabinet queries have done their best to sell that idea to the courts, and they've largely failed. The court with the most familiarity with the statute, the FISC, has consistently and expressly rejected such a requirement. (One judge in New York, has held that a 702 query requires a warrant but the judge did not exclude evidence obtained through the query and the ruling is still on appeal.)

Worse, proponents are trying to impose their vague and sweeping warrant requirement well beyond the alleged abuses it is supposed to cure. It is true that the FBI failed to follow its own rules in accessing 702 data. But the FBI's access is limited to a database containing the

communications of roughly 3% of 702 targets. The remaining data is held by, and crucial to, agencies like the CIA, NSA, and NCTC that have seen no systematic abuses. Yet the Biggs amendment, which in the last Congress would have imposed a warrant requirement on 702 searches, was drafted to impose the same unworkable warrant procedures on every intelligence agency. The changes to 702 that did pass in the last Congress appear to have worked; they imposed a detailed set of reforms to the querying process, and there's been no showing of any further abuses or problems of significance since they were adopted.

A warrant requirement is not a reform intended to prevent abuses. It's an ideological project, sweeping and formless. It is untethered to either the Constitution's requirements or to any real-world abuse. And it poses long-term dangers for our foreign intelligence capabilities.

2. **If Congress were to impose a warrant on certain US person queries beyond what is required by the Fourth Amendment, what are measures that could be included to mitigate negative impacts to national security if Congress imposed a warrant requirement?**

First, I would certainly not impose additional restrictions on searches by other intelligence agencies, which currently nominate and query data on 97% of 702 targets. But unduly restricting FBI access is dangerous; the hard lesson of 9/11 and the Wall is that agencies other than the FBI are often reluctant to look closely at U.S. persons for fear of political criticism.

So, second, we must also ensure that FBI agents can conduct legitimate 702 queries without risking their careers. It's worth noting that the Biggs amendment from last Congress would not have required warrants for queries seeking only metadata (e.g., the identities of caller and called party but not the content of the call). An approach that clearly exempts metadata access from any warrant requirement could offer certainty for the great bulk of queries, and it should allow agents to conduct such queries with fewer restrictions than at present. (It might also, however, require architectural changes to the FBI's database.)

Third, if probable cause and a warrant is to be required to review the contents of a call, it's essential to answer the question, "Probable cause to believe what?" Agents responsible for intelligence matters should not be required to show probable cause to believe that their queries are likely to turn up evidence of a crime. It might be more appropriate to require probable cause to believe that the queries will produce information relevant to a particular national security investigation or intelligence priority, but only if we are sure such a standard won't derail legitimate intelligence collection.

Fourth, it's important to allow queries to go forward without waiting for a warrant in emergencies.

Finally, if a warrant requirement is imposed, it is essential to review the access rules and the administrative enforcement procedures adopted in recent years; many would be rendered redundant if a warrant requirement is adopted, and keeping them in place would impose conflicting and confusing obligations on FBI agents

3. **Please describe the dangers of having a wall between intelligence and law enforcement and why information sharing between the two is essential.**

I described those risks in my testimony. The wall you mention was created in the 1990s. Even then, FISA was viewed with suspicion on both the left and the right. Critics claimed that it made national security wiretaps too easy, so that the government could use FISA as a back-door way of gathering criminal evidence. To reassure the critics, the Justice Department declared that a "wall" would separate national security and law enforcement investigations. Over time, the wall grew higher. By the summer of 2001, aggressive enforcement by FISA Court Chief Judge Lamberth and others had turned the wall into a no-go zone for agents who valued their careers. That same summer, in August 2001, an FBI agent learned from intelligence sources that an al-Qaeda terrorist had entered the United States. The only task force with the resources to find the terrorist was investigating the bombing of the USS Cole – as a federal crime. But to get their help would mean sending intelligence over the wall, and FBI's lawyers wouldn't allow it. The FBI's underpowered intelligence arm had weeks to find Khalid al-Mihdhar but without the Cole task force's resources, it didn't learn where he was until his team of hijackers flew American Airlines Flight 77 into the Pentagon. Thousands of Americans died that day because measures meant to protect civil liberties had left FBI agents afraid to share intelligence with law enforcement agents.

Now, 25 years later, the same thing could happen with 702. Even if 702 is renewed, the enforcement measures already in place need to be reviewed to make sure that they have not already had that effect.

4. **In your opinion, is the potential for abuse more likely under Title I or Section 702?**

Beyond doubt, Title I has been abused more outrageously than 702. The FISA order on Carter Page was so error-filled, and the errors were so consistently skewed against Donald Trump and his supporters that a fair-minded observer would be hard-pressed to call it anything but a partisan use of FISA.

The temptation to misuse Title I is built into the law. In the right circumstances, Title I offers a choice opportunity to directly target and potentially compromise political rivals. That's because it allows investigators to offer evidence that an American citizen is an agent of a foreign power and then collect every call, email, and text the target sends or receives. Title I is designed to ensure that its targets have no secrets.

Until recent reforms were imposed by Congress, the main protection against abuse of Title I was a requirement that the FISA Court approve an order based on probable cause. The irony in the current debate over imposing a warrant requirement on 702 is that this is precisely the safeguard that failed so badly in the Page case. Four judges on the FISA Court reviewed and approved the Page order, even though the underlying probable cause was weak at the start and downright laughable by the time the last two orders were approved. This is why I am so skeptical of a warrant requirement for 702; it adds burden to vital intelligence work without being tailored to prevent abuse.

702, in contrast, is much less attractive to a budding authoritarian as a tool for attacking political rivals. Most significantly, it is unlawful to target any American for surveillance under 702. Moreover, 98% of queries turn up no derogatory information, so an agent seeking to dig dirt with 702 has to take the risk of revealing his focus on a political target without much prospect of actually getting any dirt. The odds of a payoff are fifty to one. And even if his partisan target is in the database, a query will disclose only the target's communications with foreign spies, terrorists, and other intelligence targets – almost certainly a tiny slice of the target's life, and not necessarily the best place to be digging for dirt. Finally, to be candid, the justifications that must be provided for the query, plus the oversight and audits a query now triggers, particularly for sensitive matters with a political valence, add up to far more practical protection against abuse than the FISA court provided to Carter Page; indeed, we have those protections because the FISA Court's review of the Page orders was so lackadaisical that the last Congress quite properly ordered additional safeguards.

Answers to Question from Senator Amy Klobuchar

1. **Do you agree that FISA Section 702 lapsing in April presents an urgent issue that the Intelligence Community should be engaged with policymakers on addressing?**

I could not agree more. Past efforts to renew 702 began much earlier, because members of Congress all have understandable questions and suspicions about 702, many of which can only be answered in one-on-one or small-group classified briefings. Congressional willingness to support bipartisan legislation, on national security or any other topic, is weaker than at any time since 1945. A major effort by the intelligence community is essential if the partisan divide is to be overcome.

To put it another way, if I had any hair, it would already be on fire over how late it is for the intelligence community to engage.

Answers to Questions from Senator Chris Coons

1. **In your testimony, you argued that due to the recent reforms to the FBI's Section 702 querying procedures, U.S. person query numbers might be dropping because agents are hesitant to run queries or because doing so is too burdensome. You wrote that the FBI's "702 queries have fallen like a stone over four years . . . . suggest[ing] that the effort to discourage FBI agents from conducting US person 702 queries may be overachieving." You further stated that "the new measures have greatly reduced noncompliant queries, but at the cost of making Section 702 look more and more like a law enforcement 'no-go zone.'"**

    a. **What legislative reforms to Section 702 should Congress consider to ensure that agents do not run extraneous or unfounded queries but also are not prevented from running appropriate queries?**

The risk that we are deterring appropriate queries is real, and it deserves further investigation. The latest IG report suggests that risk aversion is already at work, but the evidence is not

conclusive. If deterrence and risk aversion are found, a few steps could be taken to restore a balance between deterring wrongful queries and encouraging proper ones. First, Congress and the Justice Department could explicitly distinguish between improper queries and good-faith errors and make clear that good-faith errors will not be penalized. Second, the FBI's technology architecture and access rules should allow more limited queries, such as those asking simply if there is relevant data in the database (what I call "hit-no-hit" queries), or asking only for metadata. The drafters of the Biggs amendment recognized that metadata queries should not require a warrant; they have fewer privacy implications, so less aggressive safeguards are needed. One possibility would be to adopt rules and technology that allow a "staircase" of escalating queries – from "hit-no hit" to metadata-only to full communications content, with stricter safeguards and predicates at each step.

2. **Do you think Congress should close the "data broker loophole" by which the government can circumvent restrictions by purchasing Americans' data directly from private companies that hold it?**

I do not support legislation that would impose greater restrictions on the U.S. government's access to personal data than on the private sector or foreign governments using private sector cut-outs. Efforts to enforce such a two-tier system would impose potentially sweeping and unpredictable limits on intelligence collection.

I understand the argument that private sector use of personal data is less likely to result in arrest or prosecution than government use. But government access to such data is also likely to serve a far more important societal goals than optimizing advertising yields.

If we as a nation don't want certain data collected or sold, we should prohibit its collection and sale across the board.

3. **Should Congress reconsider—and if so, how—the provisions of the *Reforming Intelligence and Securing America Act* that:**

    a. **Expanded the definition of "foreign intelligence information" to include "international production, distribution, or financing of illicit synthetic drugs, opioids, cocaine, or other drugs driving overdose deaths"?**

I felt some ambivalence about this change when it was made. Drug interdiction has usually been seen more as a law enforcement mission than as an intelligence priority; at the same time, drug overdoses and addiction have been so devastating to so many that it is hard not to support measures that might reduce that toll. Now that the definition has been expanded, we should keep a close eye on how it actually works in practice.

While I firmly believe that 702 itself should be renewed permanently, there is an argument for imposing a reasonable, say five-year, term on this amendment so that its impact can be reviewed based on actual experience.

b. Allowed agencies to use Section 702 queries to vet non-U.S persons being processed for travel to the United States?

To my mind, 702 queries are entirely appropriate for vetting purposes, especially if they can be limited in the first instance to "hit-no hit" queries. For any person seeking to enter the U.S., there's a low probability that he has been in touch with, say, a foreign terrorist targeted by 702. But the consequences of mistakenly allowing that person into the country are severe. That's what vetting databases are for – identifying risks that are low probability but high consequence. I would expand 702's use for vetting.

Answers to Questions from Senator Mike Lee

1. **Should the due process and Fourth Amendment protections guaranteed to U.S. citizens depend on executive branch compliance with internal manuals and administrative procedures? Why shouldn't Congress enact statutory safeguards?**

Congress can and sometimes should enact statutory safeguards. Remember that FISA itself was a Congressional effort to impose statutory constraints on a field previously governed only by Executive Branch rules. But turning administrative rules into statute must be done with care. Sometimes, as the disastrous history of the wall shows, protections that sound good in theory turn out to undermine national security in practice. When experience shows that a measure has that effect, internal manuals and administrative procedures can be modified far more quickly than statutory restrictions. In general, that's why Congress should elevate administrative restrictions on national security surveillance to legislation only after those restrictions have proven necessary and effective.

2. **You warned that agents are now "afraid" to use Section 702. Isn't concern about violating the law—especially where constitutional rights are at stake—precisely what accountability mechanisms are designed to encourage? Why assume that reduced query volume reflects lost national security value rather than reduced misuse?**

I don't assume that the reduced query volume reflects lost national security value, but I do believe that such a dramatic drop in queries raises a fair question about whether and how much security value has been lost and whether we're creating risk aversion in the FBI workforce. The IG's most recent report shows that this is a concern among those who work with 702. We cannot ignore that possibility the way the FISA Court in 2001 ignored the risk that its aggressive enforcement of the wall would contribute to the worst terror attack in our history.

a. If violations are merely "good-faith errors," why do they disproportionately involve U.S.-person identifiers rather than foreign targets?

This claim is an artifact of the way the 702 rules are written Almost all of the rules that FBI queries can break concern queries that use U.S.-person identifiers. Put another way, 702 queries about foreign targets rarely violate the query rules because the rules are much tougher on queries about U.S. persons.

3. **You acknowledged that some queries involving January 6 suspects or Black Lives Matter activists suggested improper motives, yet you also assert that none of the Section 702 queries that violated the rules has been flagged as undertaken with malice or intent to harm innocent Americans. Are you suggesting we should excuse improperly motivated searches simply because they happened to target people you consider guilty? Or do you believe that politically motivated queries targeting disfavored groups do not constitute malice or intent to harm?**

I appreciate the opportunity to reject the obnoxious notion that I would excuse improperly motivated searches simply because they target people I consider guilty or because targeting disfavored groups doesn't constitute malice or intent to harm. Neither is true, as my testimony made clear when I said that the nature of some queries "suggested that they might have had an improper motive."

But I also noted that vast numbers of 702 queries were launched on a routine, "just in case" basis – the way a police officer doing a traffic stop checks a driver's license with the DMV – and not out of malice or intent to harm. Given the inflammatory rhetoric around the J6 and BLM queries, I have no doubt that we would have heard if there were the slightest additional evidence that they were motivated by malice, bias, or intent to harm, as opposed to the "just in case" mindset that seems to have driven all the other queries. Since no such evidence has turned up, it's fair to conclude that those searches were good-faith errors.

4. **Your written testimony analogizes Section 702 to driver's license records. But the DMV stores records on almost every American, whereas Section 702 is intended to collect foreign intelligence, not domestic records. Doesn't that undermine the analogy at the outset?**

No it doesn't. One of the purposes of 702 is to identify foreign terrorists who are talking to Americans. One of the purposes of DMV records is to identify people driving without licenses. So it is important that traffic police know when they've encountered someone without a license and that officials charged with protecting against terrorism know when they've encountered someone who's in touch with foreign terrorists. In each case, a query to the relevant database is the best way to serve that purpose.

   a. **When law enforcement queries DMV records, it searches records collected about a specific individual. Section 702 queries search communications incidentally collected about someone else. Isn't that a material constitutional difference?**

No. There are plenty of routine searches that aren't limited to databases collected about the individual whose name is being queried. In my testimony I mentioned searches of data on stolen vehicles and ballistics. Even more on point, and fatal to the claim of a constitutional difference, is the FBI's database of criminal investigative records, which is designed to allow investigators to search records gathered in apparently unrelated cases for the names of persons of interest in their own investigation. The National Data Exchange allows searches for named U.S. persons of

criminal justice records gathered by other investigators for other purposes. This is no different from a 702 query, and no one thinks that such searches require a warrant, because the data has already been lawfully collected and stored by government agencies.

b. Private communications are also substantively different from DMV records, which are often public. Don't private communications—even with foreign nationals—carry a reasonable expectation of privacy that triggers Fourth Amendment protection?

Of course private communications deserve more protection than information voluntarily submitted to the government. But that protection has always been provided when the communications are first collected and stored, not at random intervals afterwards when the information is retrieved or examined. Section 702 requires a variety of predicates, substantive and procedural, before a foreign target's communications are collected. It's worth pointing out that communications run in two directions, so, by definition, any order allowing access to a foreign target's telephone calls will also disclose what is said by the US person he calls. Under current law, once the government has access, the cat is out of the bag.

If Congress wanted to add an unprecedented second warrant to that access, where would it begin? Would the agent who originally asked for access to the communications of a foreign terrorist need a second warrant to listen to both sides of the conversation while it is happening? Would he need a second warrant to go back the next day to listen to both sides again? Would he need a warrant to give a coworker access the day after that? None of that is required by the Fourth Amendment, and for good reason. It's unworkable and unnecessary.

It also flies in the face of nearly a century of rulings allowing law enforcement wiretaps that, more or less by definition, collect the communications of two people, one of whom was probably not identified as a surveillance target. The second speaker's words, however, may be captured as "incidental collection," and they can be reviewed, stored, and queried without a warrant. Legislation that draws that principle into question is too radical for me.

5. You say a U.S.-person query is unlikely to return a hit unless the person is "up to no good." How would an innocent American ever know—or be able to challenge—that determination? They wouldn't, because they would never be notified and never have their day in court. Correct?

The Fourth Amendment doesn't require that the targets of a search have "their day in court" before the search, since many suspects would hide evidence if they got notice that a search was in the offing. Instead, our system relies on careful scrutiny of the grounds for search. That's what the Fourth Amendment's warrant requirement does, but it's also what the various administrative reviews, audits, training, and disciplinary measures do in the context of 702. Similarly, the targets of an ordinary search and a 702 query can both challenge the use of evidence obtained through a search or a query they consider improper.

In general, the Fourth Amendment doesn't require that the target of a search get notice of a search, at least when providing notice would compromise an ongoing investigation. For the same

reason, the subject of a 702 query could not be given notice of the query without tipping off the foreign intelligence target and compromising what's likely to be a long-term surveillance.

6. **You describe agents conducting "just-in-case" searches as routine police work. Isn't that precisely what Congress has sought to prevent—transforming a foreign-intelligence authority into a domestic fishing tool?**

This is the kind of reasoning that led to the wall between law enforcement and intelligence – and to three thousand American dead. I reject it categorically.

What's more, it raises fears of abuse that simply aren't realistic. As I have made clear in answer to other questions (e.g., Chairman Grassley's question 4, above) and in my testimony, 702 queries are about as useful a "domestic fishing tool" as a rusty coffee can. It's not impossible to catch something with either, but the odds are heavily against it. And, at least in the case of 702 queries, existing safeguards virtually guarantee that the whoever is doing the fishing will soon be hearing from the game warden.