Congress of the United States
Washington, DC 20515

August 10, 2026

Orice W. Brown
Acting Comptroller General
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Acting Comptroller General Brown:

We write to request that the Government Accountability Office (GAO) conduct a comprehensive review of federal agencies' surveillance of Americans' bank accounts and financial records and identify ways to strengthen safeguards for Americans' financial privacy.

Americans' financial records can reveal deeply sensitive information including their religion; the political causes and non-profit organizations they support, including through membership; the doctors' offices and clinics where they are treated; where they travel and with whom; and countless other private personal details. Despite the sensitivity of this data, Americans' financial records receive few protections against government surveillance and existing legal authorities have at times been abused or stretched beyond their intended purpose.

There are multiple ways that federal law enforcement agencies currently surveil Americans' financial records. Accordingly, we request that GAO investigate and evaluate each of the following practices:

First, federal law enforcement agencies can force banks to disclose existing records of specific customer accounts with a subpoena, which many law enforcement agencies can issue without court review or approval. Under the Right to Financial Privacy Act, the government is generally required to tell Americans when their financial records are obtained by the government. However, in practice, it seems that the government is not providing notice. In the attached letter to Congress in October 2024, the Department of Justice indicated that it did not keep track of compliance with the legal requirements for notice. We request that GAO review federal law enforcement agencies' compliance with the Right to Financial Privacy Act's notice requirements, evaluate DOJ's recordkeeping regarding such compliance, and identify the extent to which Americans are being left uninformed when their records are seized.

Second, the Federal Bureau of Investigation (FBI) can obtain historical financial records using National Security Letters (NSLs) without prior judicial review. Under the FBI's 2016 guidelines—adopted pursuant to the USA FREEDOM Act—a nondisclosure requirement is not the default; it requires individualized written justification, high-level approval, and is subject to a presumption of termination at case closure or a three-year milestone. We request that GAO audit the FBI's implementation of these guidelines for financial NSLs, specifically evaluating: (1) the percentage of financial NSLs initially issued with a nondisclosure requirement and the percentage for which the requirement remains in place after the three-year milestone; (2) whether the FBI issues the required non-disclosure termination notices to financial institutions; and (3) any compliance issues discovered during internal audits.

Third, federal law enforcement agencies can force financial institutions to notify the government of each new transaction for a targeted account. Congress has not passed any laws explicitly authorizing real-time financial surveillance, and so the Department of Justice has instead sought court orders under the All Writs Act. This is the same obscure law under which the FBI controversially sought a court order forcing Apple to undermine the encryption protecting iPhone data in 2016. Very little is known about the scale of the government's use of these so-called "hotwatch" orders, which were first revealed publicly by a federal judge in 2005. We request that GAO investigate the scale, frequency, and legal justifications relied upon by the Department of Justice to obtain these "hotwatch" orders under the All Writs Act, providing clarity on how widely and from which types of financial institutions this mechanism is used for real-time monitoring.

Fourth, FinCEN and the FBI regularly rely on the Bank Secrecy Act and Suspicious Activity Reports (SARs) to identify money laundering, terrorist financing, tax evasion, human trafficking, and other serious crimes. When used as intended, these authorities provide law enforcement with valuable leads based on activity that financial institutions independently identify as suspicious. However, the FBI and FinCen have apparently directed banks to not just report suspicious activity but to also facilitate dragnet searches that sweep up unsuspicious American customers. SARs directives are not subject to judicial review and the banks are permanently gagged from telling their customers that they have turned over their customers' records to the government. We request that GAO assess the extent to which FinCEN and the FBI utilize BSA and SAR mechanisms to execute broad dragnet search directives, quantify the impact of these searches on ordinary Americans, and evaluate whether the use of informal directives to distribute search criteria is being used to circumvent the formal transmission mechanisms and particularized identifier requirements of Section 314(a) of the USA PATRIOT Act or oversteps FinCEN's statutory mandate to restrict its guidance to macro-level strategic advisories.

Given the potential for systemic overreach and the erosion of Americans' privacy, it is critical that Congress and the public obtain a transparent accounting of these programs. To that end, we request that GAO compile its findings into a formal report, including specific recommendations for legislative or executive reforms to ensure appropriate judicial oversight, protect innocent Americans, and enforce statutory notice requirements.

Thank you for your attention to this important matter.

Sincerely,

Ron Wyden
United States Senator

Warren Davidson
Member of Congress

Pramila Jayapal
Member of Congress

Andy Biggs
Member of Congress

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General *Washington, DC 20530*

The Honorable Ron Wyden
United States Senate
Washington, DC 20510

Dear Senator Wyden:

This responds to your letter to the Department of Justice (Department), dated April 19, 2022, regarding protective preclusion-of-notice orders issued under 18 U.S.C. § 2705(b) of the Stored Communications Act (protective orders). We apologize for our delay in responding to your letter. We are sending an identical response to the other Member who joined your letter.

The Department shares your concern that protective orders be used only for appropriate purposes, as authorized by Congress, to ensure that a provider's ability to inform its users when the government accesses personal data is not unnecessarily constrained. For this reason, the Department has issued binding national policies guaranteeing that its use of these orders meets and exceeds the standards set by Congress.

By way of background, protective orders are critical tools in criminal and national security investigations. As you noted in your letter, secrecy during an investigation may be appropriate to protect the life or physical safety of an individual or prevent the destruction of or tampering with evidence. These orders further prevent criminals, terrorists, and nation-state actors from learning of criminal investigations at a time when they could destroy evidence, harm witnesses, flee from prosecution, or adjust their behavior to defeat the Department's investigative efforts and the U.S. Intelligence Community's intelligence gathering. For example, in a child sexual abuse material investigation, a protective order may be essential to prevent an abuser from deleting or encrypting evidence before he is apprehended. In an investigation into a foreign hacker, a protective order may prevent the hacker from knowing that the United States is aware of his criminal activity, and thus that he should avoid travel to a country where he could be apprehended.

In 2017, the Department issued a policy regarding applications for protective orders under 18 U.S.C. § 2705(b).[1] Among other features, this policy requires prosecutors to only seek protective orders under compelling circumstances and after making a thorough, individualized assessment regarding the need for a protective order. It also requires prosecutors filing protective

[1] *Policy Regarding Applications for Protective Orders Pursuant to 18 U.S.C. § 2705(b),* issued October 19, 2017, available at https://www.justice.gov/criminal/criminal-ccips/page/file/1005791/dl.

order applications to seek a delay of notice of one year or less, barring exceptional circumstances. The Department supplemented this policy in May 2022, to further ensure that prosecutors make appropriate use of § 2705(b).[2] For example, before seeking a protective order greater than one year, prosecutors must notify the Department's Criminal Division or National Security Division. Subsequent applications that would create more than 18 months of cumulative delay now require a supervisor's written approval. The policy also directs every Department component to establish a protocol by which outstanding protective orders are reviewed as part of case closing procedures.

In your letter, you ask what steps the Department has taken to ensure prosecutors are complying with its § 2705(b) policy. When the policy was issued in 2017, it was distributed to all Department litigating components and U.S. Attorney's Offices. It also is regularly addressed in the Department's trainings related to electronic evidence, such as the Department's Electronic Evidence seminar. Further, it is now included in the Department's Justice Manual, which sets forth a variety of rules for federal prosecutors along with other Department policies and practices in obtaining evidence.[3] In addition, the May 2022 supplements to the policy were widely distributed and included in the Justice Manual. Procedures mandated by the supplements to the § 2705(b) policy, such as the written supervisory approval and new internal notification requirements, also help ensure that prosecutors comply with the policy.

Your letter also asks what measures the Department has in place to curtail overuse and abuse of protective orders. The Department's § 2705(b) policy itself provides for the use of protective orders only in justified circumstances. Moreover, the law associated with protective orders contains additional features that help ensure protective orders are issued only in appropriate circumstances. The statutory standard for protective orders is demanding: The government must establish that "there is reason to believe that notification of the existence of [the legal process] will result in" specified adverse circumstances, including "endangering the life or physical safety of an individual" and "seriously jeopardizing an investigation." A protective order must be issued by a court, and judicial scrutiny ensures that the Department is held to that standard in every application. As an additional safeguard, providers have the right to challenge a § 2705(b) protective order in court, and courts have applied strict scrutiny to the issuance of protective orders.[4] In combination with the § 2705(b) policy, these legal requirements guard against the unwarranted use of protective orders. Finally, the Department regularly evaluates its policies and procedures for possible improvements, as recent changes demonstrate, and it will continue to do so.

---

[2] *Supplemental Policy Regarding Applications for Protective Orders Pursuant to 18 U.S.C. 2705(b),* issued May 27, 2022, available at https://www.justice.gov/dag/file/1221126-0/dl?inline.

[3] Justice Manual § 9-13.700.

[4] See*,* e.g., In re Subpoena 2018R00776, 947 F.3d 148, 156-59 (3d Cir. 2020), citing United States v. Marcavage*,* 609 F.3d 264, 286 (3d Cir. 2010) (quoting ACLU v. Mukasey, 534 F.3d 181, 190 (3d Cir. 2008)) (indicating that strict scrutiny requires the government to demonstrate that the restriction on speech "(1) serve[s] a compelling governmental interest; (2) [is] narrowly tailored to achieve that interest; and (3) [is] the least restrictive means of advancing that interest.").

In addition, your letter asks what steps the Department takes to comply with its statutory notice obligations under both the Wiretap Act and Right to Financial Privacy Act, as well as how many individuals the Department has provided notice to under these statutes during the past three years. Inventory notice obligations under the Wiretap Act are regularly addressed in the Department's trainings related to electronic surveillance. Moreover, the Justice Manual directs prosecutors to follow the Right to Financial Privacy Act procedures, if they are to obtain customer financial records from a financial institution without alerting the target of the investigation.[5] The Department does not compile statistics regarding notice under these Acts, so we are unable to answer that portion of your questions.

More generally, in carrying out criminal law enforcement responsibilities, prosecutors are guided by the Department's Principles of Federal Prosecution (Principles) in the Justice Manual. These Principles ensure that an individual's rights are scrupulously protected while the general purposes of criminal law are adequately met. The individual's rights include those protected under the Stored Communications Act, the Wiretap Act, and the Right to Financial Privacy Act, as discussed above. Pursuant to the Principles, prosecutors commence or recommend federal prosecution only if they believe that the conduct at issue constitutes a federal offense; and the admissible evidence will probably be sufficient to obtain and sustain a conviction. Even so, the Principles provide that a prosecutor will not commence a prosecution if 1) that the prosecution would serve no substantial federal interest; 2) the individual is subject to effective prosecution in another jurisdiction; or 3) there is an adequate noncriminal alternative to prosecution. These steadfast Principles promote reasoned exercise of prosecutorial authority and contribute to fair and evenhanded administration of the federal criminal laws.

We hope this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,

Ted Schroeder
Deputy Assistant Attorney General

[5] Justice Manual § 9-13.800.