

NDO FAIRNESS ACT

MAY 15, 2023.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. JORDAN, from the Committee on the Judiciary,
submitted the following

R E P O R T

[To accompany H.R. 3089]

The Committee on the Judiciary, to whom was referred the bill (H.R. 3089) to amend title 18, United States Code, to modify delayed notice requirements, and for other purposes, having considered the same, reports favorably thereon without amendment and recommends that the bill do pass.

CONTENTS

	Page
Purpose and Summary	1
Background and Need for the Legislation	2
Committee Consideration	8
Committee Votes	8
Committee Oversight Findings	9
New Budget Authority and Tax Expenditures	9
Congressional Budget Office Cost Estimate	9
Committee Estimate of Budgetary Effects	9
Duplication of Federal Programs	9
Performance Goals and Objectives	9
Advisory on Earmarks	10
Federal Mandates Statement	10
Advisory Committee Statement	10
Applicability to Legislative Branch	10
Section-by-Section Analysis	10
Changes in Existing Law Made by the Bill, as Reported	12

Purpose and Summary

H.R. 3089, the NDO Fairness Act, introduced by Rep. Scott Fitzgerald (R-WI), would amend Title II of the Electronic Communications Privacy Act, known as the Stored Communications Act. The bill sets limits on when a governmental entity may delay notifying an individual after accessing the individual's private electronic communications (e.g., email) and after a governmental entity ob-

tains a nondisclosure order for a service provider to prevent the service provider from notifying the individual that their data has been subpoenaed.

Background and Need for the Legislation

A. BACKGROUND

i. The Stored Communications Act

In 1986, Congress enacted the Electronic Communications Privacy Act (ECPA) to prevent unauthorized government access to private electronic communications (e.g., email). Title II of the ECPA, the Stored Communications Act (SCA), focuses on the privacy of, and government access to, stored electronic communications—often in the possession of companies like Google, Apple, Microsoft, or Verizon.¹

Two key parts of the SCA are now codified in sections 2703 and 2705 of title 18. Under section 2703, if the government issues a subpoena, obtains a search warrant, or obtains a court order, the government may access the contents of electronic communications held by a service provider, in some cases without providing notice to the person whose communications are being seized and examined.² Section 2703(d) authorizes a court to order a service provider to produce electronic communications to the government if the government has shown specific and articulable facts sufficient to establish reasonable grounds to believe that the contents it seeks are relevant and material to an ongoing criminal investigation.³ However, some courts have held that this “reasonable grounds” standard is less strict than “probable cause” and may be constitutionally insufficient in some circumstances.⁴ In addition, subsection 2703(d) “does not even require a prosecutor to provide facts justifying the need for secrecy. The template merely blindly asserts that any disclosure would ‘seriously jeopardize’ the investigation for a variety of boilerplate reasons.”⁵

Section 2705 consists of two central parts. Subsection (a) authorizes the government to delay providing notice to a subscriber for up to 90 days, which may be extended repeatedly, if the government shows that there is “reason to believe” that notification may have an adverse result (e.g., danger to safety, or destruction of evidence).⁶ Orders signed by some judges may only include “a cursory assertion that the government has satisfied any or all of the statutory factors authorizing secrecy.”⁷ Subsection (b) allows for additional secrecy by prohibiting the service provider from disclosing the government’s access to anyone and subsection (b) does not limit

¹ 18 U.S.C. § 2701–2712.

² 18 U.S.C. § 2703.

³ 18 U.S.C. § 2703(d).

⁴ Charles Doyle, *Privacy: An Overview of the Electronic Communications Privacy Act*, at 42, CONG. RESEARCH SERV., (Oct. 9, 2012); *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010).

⁵ *Secrecy Orders and Prosecuting Leaks: Potential Legislative Responses to Deter Prosecutorial Abuse of Power: Hearing Before the H. comm. on the Judiciary*, 117th Cong. (2021) (written testimony of Tom Burt, Corporate Vice President, Customer Security & Trust, Microsoft Corp. at 3).

⁶ 18 U.S.C. § 2705(a).

⁷ *Secrecy Orders and Prosecuting Leaks: Potential Legislative Responses to Deter Prosecutorial Abuse of Power: Hearing Before the H. comm. on the Judiciary*, 117th Cong. (2021) (written testimony of Tom Burt, Corporate Vice President, Customer Security & Trust, Microsoft Corp. at 3).

the duration of a nondisclosure order. The nondisclosure order may be issued for “such period as the court deems appropriate.”⁸ This open-endedness means that a service provider could be indefinitely prohibited from notifying affected customers about the government’s access to private user data.

ii. Overview of Nondisclosure Orders and Department of Justice Policies and Procedures

a. The Department of Justice’s Use of Nondisclosure Orders

The Department of Justice’s (DOJ) excessive use and potential abuse of nondisclosure orders is rampant and an ongoing issue. The DOJ often uses court orders to prohibit service providers from notifying their customers that the government has seized their emails and other private information. Service providers are then left with little to no recourse to contest the orders, because it is up to the court as to when, if ever, to remove the order. At times, courts grant orders “even for routine investigations without any meaningful analysis of either the need for secrecy or the orders’ compliance with constitutional rights.”⁹ According to Microsoft, “federal law enforcement has consistently presented [the company] with 2,400 to 3,500 secrecy orders each year, or 7–10 per day, representing one-quarter to one-third of all the legal demands [it] received.”¹⁰

b. DOJ Policies and Procedures

Under the Trump Administration, in October 2017, then-Deputy Attorney General Rod Rosenstein issued a memorandum to DOJ law enforcement components and prosecutors that outlined the policies required to obtain nondisclosure orders pursuant to section 2705(b).¹¹

According to the memorandum, prosecutors who apply for nondisclosure orders must follow several steps:

1. conduct an individualized and meaningful assessment of need;
2. tailor the application to include the factual basis that identifies the need for a gag order, including the potential for data destruction, risk of flight, or risk of harm to the public;
3. prosecutors may seek a single order that covers multiple grand jury subpoenas issued as part of the same investigation;
4. unless justified by exigent circumstances, prosecutors may only seek to delay notice for up to one year;
5. the judge may direct abbreviated or lengthier periods for orders; and
6. subsequent extensions may be sought if the factors justifying protection remain.¹²

⁸ 18 U.S.C. § 2705(b).

⁹ *Secrecy Orders and Prosecuting Leaks: Potential Legislative Responses to Deter Prosecutorial Abuse of Power: Hearing Before the H. Comm. on the Judiciary*, 117th Cong. (2021) (written testimony of Tom Burt, Corporate Vice President, Customer Security & Trust, Microsoft Corp. at 2).

¹⁰ *Id.* at 3–4.

¹¹ Memorandum on Policy Regarding Applications for Protective Orders Pursuant to 18 U.S.C. § 2705(b), U.S. DEPT OF JUSTICE (Oct. 2017).

¹² *Id.*; DOJ Manual 9–13.700—Applications for Protective Orders Pursuant to 18 U.S.C. § 2705(b).

These policies were also added to the DOJ's current *Justice Manual*.

iii. DOJ Subpoenas During Leak Investigations

On June 10, 2021, the *New York Times* reported that DOJ prosecutors issued a grand jury subpoena on February 6, 2018, to Apple for data from 73 phone numbers and 36 email addresses as part of a wide-ranging investigation into the sources behind leaks of classified information related to the debunked Russia collusion investigation and other national security matters.¹³ Twelve accounts included those connected to the House Permanent Select Committee on Intelligence (HPSCI), including the former Ranking Member and a former Committee member, along with some of their staff, former aides, and family members.¹⁴ The *Times* also reported that in 2017, DOJ sent Microsoft a subpoena related to a personal email account for a congressional staff member.¹⁵ In addition, on June 5, 2021, the *New York Times* revealed that it had been under a gag order regarding a subpoena for Google to share data of four of *Times* reporters.¹⁶

HPSCI apparently learned of the subpoena on May 5, 2021, when after a three-year gag order expired (initially issued for one year, then renewed twice), the company alerted the subjects of the subpoena.¹⁷ HPSCI members were reportedly “animated” during a DOJ briefing and tried to uncover which official initiated the investigation and subpoena.¹⁸ The former Ranking Member and former Committee member called the subpoena “an attack on the separation of powers.”¹⁹ The former Committee member claimed that records of his family members (including a minor) had been obtained.²⁰

The *Wall Street Journal* has since confirmed that DOJ obtained the data as part of its fact-gathering investigation into congressional staffers leaking classified information, rather than the lawmakers themselves being targets of the investigation.²¹ According to the reporting, “current and former Justice Department officials described the subpoena as part of a fact-gathering effort and denied that it was politically motivated.”²² The *Journal* further reported that senior DOJ officials at the time the subpoena was issued, including then-Attorney General Sessions and his deputy, Rosenstein, have said that they had no knowledge of the subpoena.²³ It

¹³ Katie Benner, et al., *Hunting Leaks, Trump Officials Focused on Democrats in Congress*, N.Y. TIMES (Jun. 10, 2021).

¹⁴ *Id.*

¹⁵ Jack Nicas, et al., *In Leak Investigation, Tech Giants Are Caught Between Courts and Customers*, N.Y. TIMES (Jun. 11, 2021).

¹⁶ Charlie Savage and Katie Benner, *U.S. Waged Secret Legal Battle to Obtain Emails of 4 Times Reporters*, N.Y. TIMES (Jun. 5, 2021).

¹⁷ Jack Nicas, et al., *In Leak Investigation, Tech Giants Are Caught Between Courts and Customers*, N.Y. Times (Jun. 11, 2021); See also, Clare Foran, et al., *Justice Department watchdog to investigate data seizure as House Democrats discuss impacts of leak probe*, CNN (Jun. 11, 2021).

¹⁸ *Id.*; See also, Manu Raju, et al., *Trump Justice Department subpoenaed Apple for data from House Intelligence Committee Democrats, sources say*, CNN (Jun. 10, 2021).

¹⁹ Rebecca Heilweil, *The Trump administration forced Apple to turn over lawmakers' data. Democrats are outraged*, VOX (Jun. 14, 2021).

²⁰ Manu Raju, et al., *Trump Justice Department subpoenaed Apple for data from House Intelligence Committee Democrats, sources say*, CNN (Jun. 10, 2021).

²¹ Aruna Viswanath and Sadie Gurman, *Trump Justice Department's Leak Probe Wasn't Aimed at Lawmakers*, WALL ST. J. (Jun. 23, 2021).

²² *Id.*

²³ *Id.*

is unknown whether prosecutors had obtained the necessary approval to issue the subpoena. In 2018, the DOJ prosecuted Senate Intelligence Committee staffer James Wolfe for leaking non-public information about Committee matters to reporters.²⁴

a. Response from Trump-era DOJ officials

On June 11, 2021, during a *Politico* interview, former Attorney General William Barr said that he was not aware that any Members' records were obtained in a leak probe, pointing to the fact that cases that the Attorney General weighs in on would have been recommended by career officials in the Criminal Division and elsewhere in the Department.²⁵ He added that President Trump never directed him to target lawmakers for investigation, saying that President Trump "was not aware of who we were looking at in any of these cases. I never discussed the leak cases with [President] Trump. He didn't really ask me any of the specifics."²⁶ Likewise, according to *Business Insider*, former Attorney General Sessions and his deputy Rod Rosenstein have denied knowledge of the subpoena.²⁷

b. Congressional response to the news about DOJ's subpoenas

In response to the reporting, then-House Speaker Nancy Pelosi denounced the investigation, saying, "These actions appear to be yet another egregious assault on our democracy waged by the former president."²⁸ On June 14, 2021, Democrat Members of the Senate Judiciary Committee wrote Attorney General Garland for more information, including copies of the subpoenas and more details on the Office of Legal Counsel's approval.²⁹ That day, Attorney General Garland said that he directed his deputy Lisa Monaco to bolster the Department's procedures for obtaining records from Members of Congress, specifically "to evaluate and strengthen the department's existing policies and procedures for obtaining records of the legislative branch."³⁰ However, actions by the DOJ and FBI against Project Veritas have raised serious concerns about the enforcement of the policy that Attorney General Garland implemented—and President Biden endorsed—against federal law enforcement seizing records from journalists.³¹

²⁴ Adam Goldman, et al., *Ex-Senate Aide Charged in Leak Case Where Times Reporter's Records Were Seized*, N.Y. TIMES (Jun. 7, 2018).

²⁵ *Id.*

²⁶ Manu Raju, et al., *Trump Justice Department subpoenaed Apple for data from House Intelligence Committee Democrats, sources say*, CNN (Jun. 10, 2021).

²⁷ Tom Porter, *Top Justice Department officials Sessions, Barr and Rosenstein all deny knowledge of secret subpoenas targeting Democratic lawmakers*, BUSINESS INSIDER (Jun. 13, 2021).

²⁸ *Id.*

²⁹ Letter from Richard Durbin, Chairman, S. Comm. on Judiciary, to Merrick B. Garland, Attorney General (Jun. 14, 2021).

³⁰ Press Release, Dep't. of Justice, Statement from Attorney General Merrick B. Garland, (June 14, 2021); See also, Matt Zapotosky, *Garland says Justice Department will strengthen policies for obtaining lawmakers' records*, W. POST (June 14, 2021); See also, Sadie Gurman, *After Apple Subpoenas, Justice Department Rethinks Policies on Getting Lawmakers' Records*, WALL ST. J. (June 14, 2021).

³¹ Memorandum from Atty Gen. Merrick Garland, U.S. Dep't of Justice, Use of Compulsory Process to Obtain Information From, or Records of, Members of the News Media (July 19, 2021); Eric Tucker, *Justice Dept. says it'll no longer seize reporters' records*, AP NEWS (June 5, 2021); Alexandra Jaffe, *Biden won't allow Justice Dept. to seize reporters' records*, AP NEWS (May 21, 2021).

c. The DOJ's secret actions involving Project Veritas

In the course of Project Veritas' news-gathering activities in late 2020, the organization obtained a diary purported to belong to President Biden's daughter.³² Project Veritas could not determine the legitimacy of the diary and chose not to publish its contents.³³ Instead, the organization reportedly handed over the diary to law enforcement.³⁴ Then, on November 6, 2021, FBI agents reportedly executed a search of the residence of Project Veritas founder James O'Keefe in connection with an investigation relating to the diary.³⁵ Two days prior to the raid of O'Keefe's residence, the FBI reportedly also searched the homes of two former Project Veritas associates in connection with an investigation relating to the diary.³⁶

According to O'Keefe, the Department of Justice requested that the Project Veritas journalists not disclose the existence of the warrant.³⁷ Yet, within an hour of the FBI's raid, the New York Times published a story about the search, even though the search warrant and the subject matter of the search warrant were apparently part of a grand jury investigation and should have been non-public.³⁸ The Times later published information from confidential and sensitive documents belonging to Project Veritas, including legal advice obtained relating to its news gathering activities.³⁹ On the same day, a federal judge in New York ordered the Department to stop extracting and reviewing the contents of Project Veritas materials that the FBI seized.⁴⁰ The court's order and the Times's publishing of nonpublic Project Veritas information has raised questions about whether any Department employee leaked, or contributed to the leak of, any nonpublic information as part of this investigation.

These actions also raise concerns about the enforcement of the policy that Attorney General Garland implemented just months before concerning searching and seizing records from journalists and media organizations. President Biden endorsed Attorney General Garland's prohibition, saying that it is "simply, simply wrong" to confiscate journalists' records and that he would not allow the Department to do so.⁴¹ Similarly, then-Chairman Jerrold Nadler said he was "genuinely encouraged" by Attorney General Garland's new policy and that he "look[s] forward to working with" him "to make

³²James O'Keefe, *FBI and Southern District of New York Raid Project Veritas Journalists' Homes*, PROJECT VERITAS (Nov. 5, 2021).

³³*Id.*

³⁴*Id.*

³⁵Michael S. Schmidt, et al., *F.B.I. Searches James O'Keefe's Home in Ashley Biden Diary Theft Inquiry*, N.Y. TIMES (Nov. 6, 2021).

³⁶Amy B. Wang and Devlin Barrett, *FBI searches Project Veritas associates in probe over diary purportedly belonging to Biden's daughter*, WASH. POST (Nov. 5, 2021); Michael S. Schmidt and Adam Goldman, *Project Veritas Tells Judge It Was Assured Biden Diary Was Legally Obtained*, N.Y. TIMES (Nov. 12, 2021).

³⁷James O'Keefe, *FBI and Southern District of New York Raid Project Veritas Journalists' Homes*, PROJECT VERITAS (Nov. 5, 2021).

³⁸*Id.*

³⁹Adam Goldman and Mark Mazzetti, *Project Veritas and the Line Between Journalism and Political Spying*, N.Y. TIMES (Nov. 11, 2021).

⁴⁰Order, In re Search Warrant dated November 5, 2021, 21 MAG 10685 (S.D.N.Y. Nov. 11, 2021).

⁴¹Eric Tucker, *Justice Dept. says it'll no longer seize reporters' records*, AP NEWS (June 5, 2021); Alexandra Jaffe, *Biden won't allow Justice Dept. to seize reporters' records*, AP NEWS (May 21, 2021).

certain that these changes are codified [in law] and remain the policy of the Department for years to come.”⁴²

On November 18, 2021, then-Ranking Member Jim Jordan, then-Ranking Member James Comer, and Senator Ron Johnson wrote to Attorney General Garland requesting documents and information about the FBI’s raids on residences of individuals connected to Project Veritas.⁴³ To date, the DOJ has yet to respond with documents. This silence is especially troubling considering new legal documents that show DOJ secretly accessed emails, contacts, and other information, to surveil a number of associates of Project Veritas, while circumventing legal processes and invading First Amendment protections.⁴⁴

On March 22, 2022, lawyers representing Project Veritas sent a letter to United States District Court Judge Analisa Torres, in which they noted that from November 2020 to April 2021—and to the FBI’s raids in November 2021—prosecutors used compulsory demands, including secret warrants and nondisclosure orders, to obtain materials from Microsoft such as email accounts and contacts of the group’s associates.⁴⁵ According to the letter, the government “gained unsupervised access to as many as 150,000 emails and 1,000 contacts.”⁴⁶ Prosecutors also issued nondisclosure orders to prevent Microsoft from disclosing that the government had accessed over a year’s worth of emails.⁴⁷

This unsupervised access occurred after Judge Torres approved a request to appoint a special master to review whether materials seized by the November 2021 FBI’s raids could even be used by prosecutors as evidence.⁴⁸ At the time the DOJ’s investigation was revealed publicly, Microsoft requested that the DOJ lift its gag orders to notify the associates of Project Veritas who were Microsoft’s customers. But the DOJ refused to do so until Microsoft threatened to file a lawsuit against DOJ.⁴⁹ The DOJ eventually went to court and requested that the gag orders be lifted, and the court agreed.⁵⁰

Concerned with DOJ’s actions, even the American Civil Liberties Union (ACLU) released a statement that said it was “deeply troubled by reports that the Department of Justice obtained secret electronic surveillance orders requiring sweeping disclosure of ‘all content’ of communications associated with Project Veritas email accounts, including attorney-client communications.”⁵¹ The ACLU’s statement further called for the government to “immediately suspend its review of the materials obtained pursuant to its electronic

⁴² Press Release, H. Comm. on the Judiciary, *Chairman Nadler Statement on DOJ Policy Restricting Use of Compulsory Process to Obtain Journalists’ Records*, (July 19, 2021).

⁴³ Letter from Rep. Jim Jordan et al., Ranking Member, H. Comm. on the Judiciary, to Merrick B. Garland, Atty Gen., U.S. Dep’t of Justice (Nov. 18, 2022).

⁴⁴ Letter from Paul A. Calli et. al., to the Hon. Analisa Torres, (S.D.N.Y. Mar. 22, 2022); Josh Gerstein, *Project Veritas says feds secretly accessed its emails*, POLITICO (Mar. 22, 2022).

⁴⁵ Letter from Paul A. Calli et. al., to the Hon. Analisa Torres, (S.D.N.Y. Mar. 22, 2022).

⁴⁶ *Id.* at 5.

⁴⁷ *Id.* at 2.

⁴⁸ Order, In re Search Warrant dated November 5, 2021, 21 MAG 10685 (S.D.N.Y. Nov. 11, 2021).

⁴⁹ Letter from Paul A. Calli et. al., to the Hon. Analisa Torres, (S.D.N.Y. Mar. 22, 2022); Josh Gerstein, *Project Veritas says feds secretly accessed its emails*, POLITICO (Mar. 22, 2022); Michael S. Schmidt and Adam Goldman, *Project Veritas Says Justice Dept. Secretly Seized Its Emails*, N.Y. TIMES (Mar. 22, 2022).

⁵⁰ Michael S. Schmidt and Adam Goldman, *Project Veritas Says Justice Dept. Secretly Seized Its Emails*, N.Y. Times (Mar. 22, 2022).

⁵¹ Press Release, *ACLU COMMENT ON ALLEGATIONS OF FEDERAL LAW ENFORCEMENT SECRETLY ACCESSING PROJECT VERITAS’ EMAILS*, ACLU (Mar. 22, 2022).

surveillance orders and fully disclose the extent of its actions, so that the court can consider appropriate relief.”⁵²

B. NEED FOR LEGISLATION

On June 29, 2021, in the 117th Congress, the Committee held a hearing entitled “Secrecy Orders and Prosecuting Leaks: Potential Legislative Responses to Deter Prosecutorial Abuse of Power.”⁵³ The hearing covered relevant statutes and the policies and procedures regarding excessive use of existing authorities and abuses by the Department of Justice and Federal Bureau of Investigation related to unwarranted surveillance, gag orders, and leak investigations. During the hearing, Professor Jonathan Turley advocated for “legislative and policy changes” on nondisclosure orders saying that they can “magnify abuses” and “allow[] the government to not only conduct secret searches with little required showings but also allow[] the government to then prevent others from challenging its actions to halt possible abuses.”⁵⁴ Other witnesses similarly supported reforms, particularly to the ECPA, such as eliminating indefinite secrecy orders or requiring notice to the subject of a legal demand for data upon the expiration of a nondisclosure order.⁵⁵

The government’s rampant overuse of nondisclosure orders violates fundamental constitutional rights of all Americans. Some of these orders do not contain a time limit, creating the possibility that a subject of a search may never know that the government was spying on him or her. Courts often rubber stamp these orders through a process that goes unchallenged.

H.R. 3089 would set important limits on these nondisclosure orders. The bill requires meaningful judicial review of the need for secrecy, protects important constitutional rights by ensuring that courts may only grants nondisclosure orders when necessary, limits a nondisclosure order to 90 days, only allowing for an extension if necessary, requires the government to notify the target of its non-disclosure order within five business days of the expiration of the order and to provide detailed information about the order, like the specific nature of the government’s investigation, and allows for a service provider to challenge the nondisclosure order in court.

Committee Consideration

On May 10, 2023, the Committee met in open session and ordered the bill, H.R. 3089, favorably reported, by voice vote, a quorum being present.

Committee Votes

In compliance with clause 3(b) of House rule XIII, the Committee states that no recorded votes were taken during consideration of H.R. 3089.

⁵²*Id.*

⁵³*Secrecy Orders and Prosecuting Leaks: Potential Legislative Responses to Deter Prosecutorial Abuse of Power: Hearing Before the H. Comm. on the Judiciary*, 117th Cong. (2021).

⁵⁴*Id.* (written testimony of Jonathan Turley, J.B. and Maurice C. Shapiro Professor of Public Interest Law, George Washington University Law School at 6).

⁵⁵*Id.* (written testimony of Tom Burt, Corporate Vice President, Customer Security & Trust, Microsoft Corp. at 6).

Committee Oversight Findings

In compliance with clause 3(c)(1) of House rule XIII, the Committee advises that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

New Budget Authority and Tax Expenditures

With respect to the requirements of clause 3(c)(2) of rule XIII of the Rules of the House of Representatives and section 308(a) of the *Congressional Budget Act of 1974* and with respect to the requirements of clause 3(c)(3) of rule XIII of the Rules of the House of Representatives and section 402 of the *Congressional Budget Act of 1974*, the Committee has requested but not received a cost estimate for this bill from the Director of the Congressional Budget Office. The Committee has requested but not received from the Director of the Congressional Budget Office a statement as to whether this bill contains any new budget authority, spending authority, credit authority, or an increase or decrease in revenues or tax expenditures. The Chairman of the Committee shall cause such estimate and statement to be printed in the *Congressional Record* upon its receipt by the Committee.

Congressional Budget Office Cost Estimate

With respect to the requirement of clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, a cost estimate provided by the Congressional Budget Office pursuant to section 402 of the *Congressional Budget Act of 1974* was not made available to the Committee in time for the filing of this report. The Chairman of the Committee shall cause such estimate to be printed in the *Congressional Record* upon its receipt by the Committee.

Committee Estimate of Budgetary Effects

With respect to the requirements of clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the *Congressional Budget Act of 1974*.

Duplication of Federal Programs

Pursuant to clause 3(c)(5) of House rule XIII, no provision of H.R. 3089 establishes or reauthorizes a program of the federal government known to be duplicative of another federal program.

Performance Goals and Objectives

The Committee states that pursuant to clause 3(c)(4) of House rule XIII, H.R. 3089 would establish new restrictions on a governmental entity's ability to obtain a nondisclosure order when obtaining communications from a service provider.

Advisory on Earmarks

In accordance with clause 9 of House rule XXI, H.R. 3089 does not contain any congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clauses 9(d), 9(e), or 9(f) of House Rule XXI.

Federal Mandates Statement

Pursuant to section 423 of the *Unfunded Mandates Reform Act*, the Committee has determined that the bill does not contain federal mandates on the private sector. The Committee has determined that the bill does not impose a federal intergovernmental mandate on state, local, or tribal governments.

Advisory Committee Statement

No advisory committees within the meaning of section 5(b) of the *Federal Advisory Committee Act* were created by this legislation.

Applicability to Legislative Branch

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the *Congressional Accountability Act* (Pub. L. 104-1).

Section-by-Section Analysis

Sec. 1. Short Title. Section 1 sets forth the title of this bill, the “NDO Fairness Act.”

Sec. 2. Preclusion of Notice. Section 2 amends 18 U.S.C. 2705(b) to include the following paragraphs.

- *Paragraph (1) Application.* Permits a governmental entity, when seeking access to private electronic communications, to seek a court order to direct a service provider or remote computing service not to disclose to any other person such access for a period of not more than 90 days. The application shall state whether the named customer or subscriber whose information is sought is: (1) aware of the warrant, order, subpoena, or underlying investigation; and (2) is suspected of involvement in the commission of the crime under investigation. An order may not direct, or otherwise require, a service provider or remote computing service to notify the court or government of the expiration of the order.

- *Paragraph (2) Determination.* Prohibits a court from granting a request for an order or extension unless the court: (1) determines, in writing, based on specific and articulable facts, including written findings of fact and conclusions of law, that the notification is likely to result in endangering the safety of an individual, flight from prosecution, destruction of evidence, intimidation of possible witnesses, or otherwise jeopardize an investigation or unduly delay a trial; (2) the order is narrowly tailored and there is no less restrictive alternative; and (3) the court has reviewed the individual warrant, order, or subpoena. The court may consider the nature of the offense in issuing a determination.

- *Paragraph (3) Extension.* Permits extension requests by the governmental entity for not more than 90 days for each extension and requires a court make the same paragraph (2) written determination.

- *Paragraph (4) Notification of Changed Circumstances.* Requires the governmental entity to notify the court within a reasonable period of time, not to exceed 14 days, of any material change in the need for the court order and requires the court to reexamine the order accordingly.

- *Paragraph (5) Opportunity to be Heard.* Permits a court to vacate an order upon petition by a service provider if the order does not meet the requirements under paragraph (2) or if compliance would be unreasonable or otherwise unlawful. The required disclosure would be stayed, unless the court determines otherwise, until the court issues a decision, and such decision would be a final, appealable order.

- *Paragraph (6) Exception.* Permits providers to disclose the existence of an order to those persons who are necessary for compliance, attorneys, and any other person determined by the court.

- *Paragraph (7) Scope of Nondisclosure.* Makes a person who received a disclosure subject to the same nondisclosure requirements as the person who received the order.

- *Paragraph (8) Supporting Documentation.* Requires the governmental entity to include in the service of the order to a provider a copy of the warrant, order, or subpoena to which the nondisclosure order applies.

- *Paragraph (9) Expiration of Order Precluding Notice.* Requires the governmental entity to deliver a copy of the warrant, order, or subpoena to the named customer or subscriber within 5 business days of expiration of an order or extension that precludes notice, including information about the specific nature of the government inquiry, that information was requested or provided to the governmental entity, the existence of the delay by court order, the identity of the court that authorized the delay, the legal basis for the delay, and that the governmental entity must provide upon request by the customer or subscriber a copy of the disclosed information or a written certification that no information was disclosed.

- *Paragraph (10) Copy of Information Disclosed.* Requires the governmental entity, if requested by the customer or subscriber within 180 days after expiration of the order, to provide a copy of the disclosed information (except illicit records, child sexual abuse material, and other illegal material) or a written certification that no information was disclosed.

- *Paragraph (11) Redactions.* Any information disclosed under paragraphs (9) and (10) may be redacted if a court finds it necessary to preserve the secrecy or integrity of an investigation.

Sec. 3. Additional Provisions Regarding Delayed Notice. Section 3 adds a new subsection (c) to section 2705, which would require DOJ to submit an annual report to the House and Senate Judiciary Committees and the Director of the Administrative Office of the United States Courts providing information relating to the use of section 2703 and 2705 authorities for each federal judicial district.

This information includes the number of customers or subscribers targeted for a section 2703 warrant, subpoena, or order, the number of applications for a delay of notification, preclusion of notice, and extensions, the number of granted, extended, or denied orders, the number of orders that target a member of the news media, and the total number of resulting arrests, trials, and convictions. The report would also include a description of the process and the information used to gather the data. The Administrative Office of the United States Courts is required to publish the report on its website.

Changes in Existing Law Made by the Bill, as Reported

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italics, and existing law in which no change is proposed is shown in roman):

TITLE 18, UNITED STATES CODE

* * * * *

PART I—CRIMES

* * * * *

CHAPTER 121—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

* * * * *

§ 2705. Delayed notice

(a) **DELAY OF NOTIFICATION.**—(1) A governmental entity acting under section 2703(b) of this title may—

(A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed ninety days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or

(B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed ninety days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.

(2) An adverse result for the purposes of paragraph (1) of this subsection is—

- (A) endangering the life or physical safety of an individual;
- (B) flight from prosecution;

- (C) destruction of or tampering with evidence;
- (D) intimidation of potential witnesses; or
- (E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(3) The governmental entity shall maintain a true copy of certification under paragraph (1)(B).

(4) Extensions of the delay of notification provided in section 2703 of up to ninety days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) of this section.

(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first-class mail to, the customer or subscriber a copy of the process or request together with notice that—

- (A) states with reasonable specificity the nature of the law enforcement inquiry; and
- (B) informs such customer or subscriber—
 - (i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;
 - (ii) that notification of such customer or subscriber was delayed;
 - (iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and
 - (iv) which provision of this chapter allowed such delay.

(6) As used in this subsection, the term “supervisory official” means the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency’s headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney’s headquarters or regional office.

[(b) PRECLUSION OF NOTICE TO SUBJECT OF GOVERNMENTAL ACCESS.]—A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—

- [(1)]** endangering the life or physical safety of an individual;
- [(2)]** flight from prosecution;
- [(3)]** destruction of or tampering with evidence;
- [(4)]** intimidation of potential witnesses; or
- [(5)]** otherwise seriously jeopardizing an investigation or unduly delaying a trial.**]**

(b) PRECLUSION OF NOTICE.—

(1) APPLICATION.—

(A) *IN GENERAL.*—A governmental entity that is seeking a warrant, order, or subpoena under section 2703, when it is not required to notify the customer or subscriber, or to the extent that it may delay such notice pursuant to subsection (a), may apply to a court for an order, subject to paragraph (6), directing a provider of electronic communications service or remote computing service to which a warrant, order, or subpoena under section 2703 is directed not to notify any other person of the existence of the warrant, order, or subpoena.

(B) *LENGTH.*—An order granted under subparagraph (A) shall be in effect for a period of not more than 90 days.

(C) *OTHER REQUIREMENTS.*—

(i) *IN GENERAL.*—A application for an order under subparagraph (A) shall state, to the best of the applicant's knowledge, whether the named customer or subscriber whose information is sought by the warrant, order, or subpoena under section 2703—

(I) is aware of the warrant, order, subpoena, or underlying investigation; and

(II) is suspected of involvement in the commission of the crime under investigation.

(ii) *ORDERS.*—An order granted under this paragraph may not direct, or otherwise require, a provider of electronic communications service or remote computing service to provide notification of the expiration of order to the court or government entity that sought the order.

(2) *DETERMINATION.*—

(A) *IN GENERAL.*—The court may not grant a request for an order made under paragraph (1), or an extension of such order requested by the governmental entity pursuant to paragraph (3), unless—

(i) the court issues a written determination, based on specific and articulable facts, and including written findings of fact and conclusions of law, that it is likely that not granting the request will result in—

(I) endangering the life or physical safety of an individual;

(II) flight from prosecution;

(III) destruction of or tampering with evidence;

(IV) intimidation of potential witnesses; or

(V) otherwise seriously jeopardizing an investigation or unduly delaying a trial; and

(ii) the order is narrowly tailored and there is no less restrictive alternative, including notification to an individual or organization within or providing legal representation to the named customer or subscriber, that is not likely to result in an adverse result as described in clauses (i) through (v) of subparagraph (A); and

(iii) the court has reviewed the individual warrant, order, or subpoena under section 2703 to which the order issued under this paragraph applies.

(B) *NATURE OF THE OFFENSE.*—The court may consider the nature of the offense in issuing a determination under subparagraph (A).

(3) *EXTENSION.*—A governmental entity may request one or more extensions of an order granted under paragraph (2) of not more than 90 days for each such extension. The court may only grant such an extension if the court makes a written determination required under paragraph (2)(A) and the extension is in accordance with the requirements of (2)(B).

(4) *NOTIFICATION OF CHANGED CIRCUMSTANCES.*—If the need for the order issued under paragraph (2) changes materially, the governmental entity that requested the order shall notify the court within a reasonable period of time (not to exceed 14 days) of the changed circumstances, and the court shall reassess the order and modify or vacate as appropriate.

(5) *OPPORTUNITY TO BE HEARD.*—

(A) *IN GENERAL.*—Upon an application, petition, or motion by a provider of electronic communications service or remote computing service or person acting on behalf of the provider to which an order under paragraph (2) (or an extension under paragraph (3)) has been issued, the court may modify or vacate the order if—

- (i) the order does not meet requirements provided in paragraph (2) or (3); or
- (ii) compliance with the order is unreasonable or otherwise unlawful.

(B) *STAY OF DISCLOSURE OF NAMED CUSTOMER OR SUBSCRIBER COMMUNICATIONS OR RECORDS.*—A provider's obligation to disclose the information requested in the warrant, order, or subpoena to which the order in paragraph (1) applies is stayed upon the filing of the application, petition, or motion under this paragraph pending resolution of the application, petition, or motion, unless the court with jurisdiction over the challenge determines based on a showing by the governmental entity that the stay should be lifted in whole or in part prior to resolution.

(C) *FINALITY OF ORDER.*—The decision of the court resolving an application, petition, or motion under this paragraph shall constitute a final, appealable order.

(6) *EXCEPTION.*—A provider of electronic communications service or remote computing service to which an order under paragraph (2) applies, or an officer, employee, or agent thereof, may disclose information otherwise subject to any applicable nondisclosure requirement to—

(A) those persons to whom disclosure is necessary in order to comply with the warrant, order, or subpoena;

(B) an attorney in order to obtain legal advice or assistance regarding the order issued under paragraph (2) or the warrant, order, or subpoena to which the order applies; and

(C) any person the court determines can be notified of the warrant, order, or subpoena.

(7) *SCOPE OF NONDISCLOSURE.*—Any person to whom disclosure is made under paragraph (6) (other than the governmental entity) shall be subject to the nondisclosure requirements appli-

cable to the person to whom the order is issued. Any recipient authorized under this subsection to disclose to a person information otherwise subject to a nondisclosure requirement shall notify the person of the applicable nondisclosure requirement.

(8) *SUPPORTING DOCUMENTATION*.—Upon serving a provider of electronic communications service or remote computing service with an order granted under paragraph (2), or an extension of such order granted under paragraph (3), the governmental entity shall include a copy of the warrant, order, or subpoena to which the nondisclosure order applies.

(9) *EXPIRATION OF ORDER PRECLUDING NOTICE*.—Upon expiration of an order issued under paragraph (2) or, if an extension has been granted under paragraph (3), expiration of the extension, the governmental entity shall deliver to the named customer or subscriber, by at least 2 methods, which shall be personal service, registered or first-class mail, electronic mail, or other means approved by the court as reasonably calculated to reach the named customer or subscriber within 5 business days of the expiration of the order—

- (A) a copy of the warrant, order, or subpoena; and
- (B) notice that informs the named customer or subscriber—

(i) of the nature of the law enforcement inquiry with reasonable specificity;

(ii) that information maintained for such customer or subscriber by the provider of electronic communications service or remote computing service to which the warrant, order, or subpoena under section 2703, was directed was supplied to or requested by the government entity;

(iii) that notification of such customer or subscriber was precluded by court order;

(iv) of the identity of the court authorizing the preclusion of notice;

(v) of the provision of this chapter under which the preclusion of notice was authorized; and

(vi) that the government will, upon request by the customer or subscriber made within 180 days after receiving notification under this paragraph, provide the named customer or subscriber with a copy of the information that was disclosed in response to the warrant, order or subpoena, or in the event that no information was disclosed, a written certification that no information was disclosed.

(10) *COPY OF INFORMATION DISCLOSED*.—Upon expiration of the order precluding notice issued under paragraph (2) or (3) of this subsection, and at the request of the named customer or subscriber made within 180 days of receiving notification under paragraph (9), the governmental entity shall promptly provide the named customer or subscriber—

- (A) with a copy of the information that was disclosed in response to the warrant, order or subpoena (except illicit records, child sexual abuse material, and other illegal material); or

(B) in the event that no information was disclosed, a written certification that no information was disclosed.

(11) REDACTIONS.—Any information disclosed pursuant to paragraphs (9) and (10) may be redacted only if a court finds such redactions necessary to preserve the secrecy or integrity of an investigation.

(c) ANNUAL REPORT.—On an annual basis, the Attorney General shall provide to the Committee on the Judiciary of the House of Representatives, the Committee on the Judiciary of the Senate, and the Director of the Administrative Office of the United States Courts, which the Director shall publish on the website of the Administrative Office of the United States Courts, in a manner consistent with protection of national security, a report setting forth with respect to the preceding calendar year, for each Federal judicial district—

(1) the number of named customers or subscribers with respect to whom, in that calendar year, a warrant, subpoena, or court order was issued pursuant to section 2703;

(2) the aggregate number of applications requesting delay of notification pursuant to subsection (a)(1), preclusion of notice pursuant to subsection (b)(1), and extensions pursuant to subsection (b)(3);

(3) the aggregate number of orders under this section either granting, extending, or denying a request for delay of notification or preclusion of notice;

(4) the aggregate number of orders under this section affecting a member of the news media, including any conduct related to activities protected under the First Amendment; and

(5) the aggregate number of arrests, trials, and convictions, resulting from investigations in which orders under this section were obtained, including the offenses for which individuals were arrested, tried, or convicted.

The Attorney General shall include in the report under this subsection a description of the process and the information used to determine the numbers for each of paragraphs (1) through (5).

* * * * *

