REPORTERS COMMITTEE SPECIAL ANALYSIS

RE: Default Notice Rules for Subpoenas, Court Orders, and Warrants Without a "Hard Backstop" in Justice Department Policies Requiring Notice to Affected Member of News Media Within 90 Days[1]

I. Introduction

For almost five decades, the Justice Department has had internal policies in place that govern when law enforcement may investigate members of the news media. Known as the "news media guidelines," these policies provide that, with respect to third-party physical and electronic search warrants, court orders, and subpoenas, the Justice Department must first notify an affected member of the news media, which gives a news organization the opportunity to challenge improper requests in court. There are only limited exceptions.

Additionally, even when those limited exceptions apply, the Justice Department may delay notifying an affected member of the news media only for a time certain: one initial 45-day period of delay (after any return under the subpoena or other legal process) and one 45-day extension.

This 90-day "hard backstop" is an indispensable protection for the news media. It ensures that journalists and news organizations find out that records that may reveal, for instance, the identities of confidential sources have been disclosed to the government. And, particularly in the context of electronic material, there are scenarios where, absent the hard backstop, journalists and news organizations might *never* find out about a third-party search or production. In other cases where the period of delay must ultimately expire, the backstop may still significantly shorten the period of possible delay.

The guidelines contain another important check: the attorney general must affirmatively determine, before authorizing delay, that negotiations with the affected member of the news media – and therefore notice of the contemplated subpoena, court order, or warrant – would risk a "clear and substantial" threat to the investigation, "grave harm" to national security, or present an "imminent threat of death or serious bodily harm."

---

[1] This special analysis is authored by Technology and Press Freedom Project Director Gabe Rottman and Stanton Foundation National Security-Free Press fellow Linda Moon.

This was a crucial innovation of the 2014-2015 changes to the guidelines; the prior versions required an affirmative determination that harm would *not* occur to *permit* notice to the affected member of the news media. The recent reform flipped that presumption.

Were the Justice Department to remove this hard 90-day backstop and argue that the notice requirements in news media investigations ought to be harmonized with existing law in other areas, the picture becomes much more complicated, particularly in the context of electronic warrants, pen register/trap-and-trace orders for the prospective collection of communications metadata ("PR-TT" orders), court orders (known as "(d)" orders) under Section 2703(d) of the Stored Communications Act ("SCA") for the retrospective collection of electronic transactional and other records, and grand jury and administrative subpoenas for basic subscriber information.

As noted, in a world without the backstop, there are scenarios where notice could effectively be delayed in perpetuity. Perpetual delay should and likely would pose First and Fourth Amendment concerns, but without notice of the search or demand for records, it is unlikely one would know enough to bring a case to end the delay. Perhaps counterintuitively, that threat may be most concerning in cases where the government has used a full SCA warrant to seize communications content from a third-party provider.

In the James Rosen case, for instance, the government argued that the plain language of the SCA permitted it to *never* notify Rosen that his emails had been seized. Former Chief Judge Royce Lamberth of the U.S. District Court for the District of Columbia disagreed with that reasoning but effectively permitted perpetual delay of the warrant by finding that any notice requirement under the federal rules was satisfied when the warrant was delivered to the third-party email vendor, in that case Google.

The Rosen warrant was signed in May 2010, and he and his employer, Fox News, found out about it after the Washington Post reported on the affidavit filed in support of the warrant application in 2013. (Interestingly, in 2010, the guidelines applied only to subpoenas, not to search warrants, and the Justice Department claimed in 2013 that it *had* provided notice to News Corp., Fox News's parent company at the time, of *subpoenas* seeking Rosen's records.)

In addition, the government is also permitted to seek gag orders with no fixed expiration that *prohibit* the third-party from notifying the subscriber that her communications or records have been seized. This practice is subject to a recent policy change that, as a matter of Justice Department discretion, limits but does not eliminate the possibility of indefinite gags.[2]

The danger with perpetual delay is that a member of the news media could have her emails, voicemails, and texts, along with her phone and electronic records, seized despite her not being the subject or target of the investigation, and she would never know.

---

2 The new policy purports to cut down on indefinite gags, but notice can still be delayed for a full year and – in "extraordinary circumstances" – for a longer period (or indefinitely). The notice preclusion orders, under 18 U.S.C. § 2705, are discussed in greater detail below.

This would most immediately imperil source confidences, including sources with no connection to the underlying investigation, and potentially sources for other reporters if the target reporter has correspondence with others in the newsroom. Additionally, the covert seizure of a reporter's inbox could raise digital security issues (for instance, where IT has provided instructions for how to communicate securely with a source or how to use systems to anonymously receive tips).

The James Wolfe leak case, in which reporter Ali Watkins had her records seized from third-party communications providers, is instructive. Absent the 90-day backstop, it's entirely possible that Watkins would not have learned that her records had been seized as part of the investigation, unless that fact had been expressly stated in Wolfe's charging documents.

The subpoenas and court order in that case would have been accompanied with a gag precluding her email and phone providers from notifying her of the seizure, and, because the demand for records was limited to non-content information, the government had no obligation (absent the guidelines) to notify Watkins of the seizure.

Additionally, while the government's sentencing memorandum includes details about how investigators seized Wolfe's records, one cannot tell from the sentencing memorandum or the government's other filings in the case that Watkins's records had also been seized.[3] Without the hard backstop, there would have been no notice requirement for the government, and the Justice Department could have conceivably secured an indefinite gag on the provider.

This is all explained in more detail below. Please note that the aforementioned distinction between when the government is *required* to notify the affected member of the news media, and when the third-party is *permitted* to tell the affected subscriber or customer, is an important one, and it can cause some confusion. Please also note that this analysis does not address national security-related investigative tools under the Foreign Intelligence Surveillance Act, the national security letter statutes, or Title III wiretaps, as they are not within the scope of the guidelines.

II. The Current Notice Provision in the Guidelines

The current version of 28 C.F.R. § 50.10 implements two major reforms from 2014-2015 relevant to the notice requirements in the guidelines.

First, it expanded the scope of covered investigative tools beyond grand jury subpoenas, including those for telephone toll records that were added in 1980, to search warrants (both traditional and under the SCA), PR-TT orders under 18 U.S.C. § 3123, and court orders for transactional and other records under Section 2703(d) of the SCA.

Second, it reversed the aforementioned presumption against notice (also added in 1980) and required the attorney general to affirmatively determine, "for compelling reasons, [that] notice would pose a *clear and substantial* threat to the integrity of the investigation, risk *grave* harm to national security, or present an imminent risk of death or serious bodily harm." 28 C.F.R. § 50.10(a)(3)-(4), (c)(4)(iv)(A), (c)(5)(iv)(A), (e)(2)(i), (e)(3) (emphasis added).

---

3 *See, e.g.*, Gov't's Sentencing Mem. and Mot. for Upward Departure and/or Variance at 12 n.9, United States v. Wolfe, 18-cr-170 (KBJ) (D.D.C. Dec. 11, 2018).

This language appears several times in the current version of the guidelines: in the statement of principles, *id.* § 50.10(a)(3)-(4); in the specific instructions for securing attorney general approval to issue subpoenas to members of the news media and third parties, *id.* § 50.10(c)(4)(iv)(A) and (c)(5)(iv)(A); and in the primary notice section, *id.* § 50.10(e)(2)(i). The guidelines also state that "the mere possibility that notice to the affected member of the news media, and potential judicial review, might delay the investigation is not, on its own, a compelling reason to delay notice." *Id.* § 50.10 (e)(2)(ii). These rules apply to warrants, court orders, and subpoenas.

The current guidelines incorporate the period of delay provisions that date back to the 1980 revisions, which were prompted by the delayed-notice seizure of phone records from Howell Raines's home phone and the Atlanta bureau of the New York Times. *See New York Times Co. v. Gonzales*, 382 F. Supp. 2d 457, 481 n.17 (S.D.N.Y. 2005), *vacated and remanded*, 459 F.3d 160 (2d Cir. 2006); Robert Pear, *Justice Dept. Restricts Subpoenas for Reporters and Phone Records*, N.Y. Times (Nov. 13, 1980), https://perma.cc/YE38-UWJB.

Under current practice, prosecutors must provide notice to the affected member of the news media as soon as they determine that the threat to the investigation, national security, or life and limb has ended. 28 C.F.R. § 50.10(e)(3). In any event, notice must be given within 45 days, and the attorney general may authorize a second 45-day delay period upon an additional determination that notice would harm the investigation, national security, or life and limb. *Id.* The guidelines permit no delays beyond the 90 days. *Id.*

Finally, the United States attorney or relevant assistant attorney general must produce a copy of the notice to be provided to the member of the news media to the Office of Public Affairs and to the Criminal Division's Office of Enforcement Affairs at least 10 business days before notice is to be given, and immediately after notice is, in fact, given. *Id.* § 50.10(e)(4).

III. How Notice Would Work in a World Without the 90-Day Backstop

The notice requirements in the physical world are slightly more straightforward than those that apply when the government has sought electronic communications content or metadata from a third-party provider.

With respect to the physical world, the basic notice rules are as follows. While notice of a warrant may be a constitutional requirement under the Fourth Amendment (courts split on the question), the federal "sneak and peek" statute permits delay and does not, by its terms, have a date certain "backstop" beyond which notice may no longer be delayed. Other types of process, including grand jury and administrative subpoenas, have notice and gag provisions that are statute specific.

Regarding electronic communications, some background on the complexities of the SCA and the Pen Register Act ("PRA") is necessary, which is provided below, following a discussion of physical search warrants and subpoenas.

Please also note that a one-page chart, attached to this paper, summarizes the discussion below and provides a quick reference to determine when notice from the government is required and how it may be delayed, and whether the government can secure a gag order to prevent a third party from notifying the target of the subpoena or other process.

a. Notice in the Physical World

i. Search Warrants

Federal Rule of Criminal Procedure 41 governs the procedures to be followed when federal law enforcement officers or attorneys for the government seek warrants for searches and seizures.

Notice is provided through the requirement that the officer executing the warrant must inventory any property seized and provide a receipt with that information and a copy of the warrant to the person from whom, or from whose premises, the property was seized (or leave the warrant and receipt at the premises). Rule 41(f)(1)(C). However, a judge may "delay any notice required by this rule if the delay is authorized by statute." Rule 41(f)(3).

The constitutionality of delayed-notice searches has been debated by the courts. In the case of wiretapping, which is analogous to a delayed-notice search, the Supreme Court in *Berger v. New York*, 388 U.S. 41, 60 (1967), struck down a New York eavesdropping law in part because of no provision for notice at some date certain. The federal wiretapping law avoids that constitutional infirmity by providing that an inventory must be returned within 90 days, though that may also be postponed on a showing of good cause and without a date certain for the inventory to be delivered. *See* 18 U.S.C. § 2518(8)(d).

So called "sneak and peek" warrants, where law enforcement covertly breaks into and searches the target premises and delays notice of the search, have likewise been upheld against constitutional challenges so long as notice is given within a "reasonable" period. Courts split on what "reasonable" means, and no court has ever addressed whether an indefinite delay would be *per se* "unreasonable" under the Fourth Amendment.[4]

For instance, in a case involving a surreptitious entry into a suspected methamphetamine production facility, the Ninth Circuit held that the warrant in that case (in which the magistrate judge had just crossed out the inventory requirement and the requirement that a copy of the inventory and warrant be left at the scene) was constitutionally defective for failing to "provide explicitly for notice within a reasonable, but short, time subsequent to the surreptitious entry." *United States v. Freitas* (*"Freitas I*") 800 F.2d at 1456 (9th Cir. 1986); *see also United States v. Freitas* ("*Freitas II*"), 856 F.2d 1425 (9th Cir. 1988) (holding no-notice warrant constitutionally infirm but declining to suppress under good faith doctrine).

---

[4] Early covert search cases suggested that seven days, with extensions possible on a new showing of cause, would be a reasonable delay for Fourth Amendment purposes. *See United States v. Freitas* ("*Freitas I*"), 800 F.2d 1451, 1456 (9th Cir. 1986); *United States v. Villegas*, 899 F.2d 1324, 1337 (2d Cir. 1990). As discussed in this section, that relatively limited period of delay has ballooned under the modern statutory framework.

By contrast, in *United States v. Pangburn*, 983 F.2d 449 (2d Cir. 2007), the Second Circuit blessed a covert search warrant without a seven-day notice requirement, rooted any notice requirement in Rule 41, not "amorphous Fourth Amendment 'interests,'" and consequently denied a motion to suppress. *Id.* at 455.

In response to this uncertainty in federal law, Congress created "sneak and peek" and "sneak and steal" warrant authority in the USA Patriot Act, Pub. L. No. 107-56, 11 Stat. 285, 213 (2001). "Sneak and steal" warrants permit police to seize tangible things when executing a covert-entry, delayed-notice warrant. (They often leave the scene looking like a burglary had taken place.)

The relevant statute, 18 U.S.C. § 3103a, authorizes delayed notice when a court finds reasonable cause to believe that one of the adverse results listed in Section 2705, mentioned above, may occur (endangering the life or physical safety of an individual, flight from prosecution, destruction or tampering with evidence, intimidation of potential witnesses, or otherwise seriously jeopardizing a trial). *Id.* § 3103a(b)(1). Note that, unlike Section 2705, an undue trial delay will *not* constitute an adverse result in the sneak and peek statute. *Id.*

The warrant also comes with other qualifications. It must:

- Prohibit the seizure of any tangible property, any wire or electronic communication, or any stored wire or electronic communication (save as provided for under the SCA), except where the judge finds "reasonable necessity for the seizure." *Id.* § 3103a(b)(2); and

- "Provide[] for the giving of such notice within a reasonable period not to exceed 30 days after the date of its execution, or on a later date certain if the facts of the case justify a longer period of delay." *Id.* § 3103a(b)(3).

However, any period of delay under Section 3103a may be extended by the court for good cause shown and an updated showing of need. *Id.* § 3103a(c). Such extensions should be limited to 90 days "unless the facts of the case justify a longer period of delay." *Id.* There is no limit on the number of extensions that may be granted.[5] Accordingly, absent the hard 90-day backstop in the guidelines, notice of any warrant could be delayed for longer than 90 days, and potentially for a significantly longer period depending on the facts of the case.

---

[5] The Administrative Office of the Courts publishes annual data on sneak and peek warrants. The most recent report shows that such warrants are most often used in drug cases. (More than 80 percent of the reported cases, in fact, are drug investigations.) Periods of delay ranged from 1 to 999 days, with the most frequently reported period of delay of 30 days. Courts reported extensions of delay ranging from 1 to 91, meaning that in one case, the court granted 91 extensions. There were more than 9,000 delayed-notice search warrant requests and more than 6,000 extension requests. The average delay in days, overall, was 84 days. *See* Report of the Director of the Administrative Office of the United States Court on Applications for Delayed-Notice Search Warrants and Extensions, https://perma.cc/EBW6-NMW5 (covering the period October 1, 2015, to September 30, 2016).

Delayed notice of a media warrant (targeted directly to a member of the news media or served on a third-party vendor of the member) raises the same concern as delayed notice generally – that the member of the news media loses the ability to challenge the warrant as improper or overbroad before it is executed. Additionally, once notice is delayed and the warrant is executed, the typical remedy for an improper warrant, suppression of any evidence produced by the defective search at trial, would be of limited utility to an affected member of the news media (as in, for instance, the Rosen case) as the affected member would not be the defendant.

ii. Grand Jury and Administrative Subpoenas

The issue of notice for the seizure of documents or business records held by a third party comes up with both grand jury and administrative subpoenas. Note that the definition of business records in the guidelines encompasses "work product and other documentary materials, including the financial transactions, of a member of the news media related to the coverage, investigation, or reporting of news." 28 C.F.R. § 50.10(b)(3)(iii)(A). They are "limited to those generated or maintained by a third party with which the member of the news media has a contractual relationship, and which could provide information about the newsgathering techniques or sources of a member of the news media." *Id.* The guidelines will therefore not protect records unrelated to newsgathering activities. *Id.* § (b)(3)(iii)(B).

With respect to whether the third-party recipient of a *grand jury* subpoena can notify the record owner, Federal Rule of Criminal Procedure 6(e) prohibits, with limited exceptions, disclosure of matters occurring before the grand jury generally, but does not gag grand jury witnesses.

That said, some courts exercising their inherent authority over grand jury proceedings will issue a protective order prohibiting witness disclosures during an ongoing investigation upon a showing of "compelling necessity." *See In re Subpoena to Testify Before Grand Jury Directed to Custodian of Records*, 864 F.2d 1559 (11th Cir. 1989); *In re Grand Jury Subpoena Duces Tecum*, 797 F.2d 676 (8th Cir. 1986); *In re Swearingen Aviation Corp.*, 486 F. Supp. 9 (D. Md.1979), *mandamus refused*, 605 F.2d 125 (4th Cir. 1979) (targets do not have standing to object to court imposed witness secrecy); *In re Grand Jury Proceedings (Fernandez Diamante)*, 814 F.2d 61 (1st Cir. 1987).

There are constitutional limits on witness gags, however. In *Butterworth v. Smith*, for instance, the Supreme Court held that to the extent a Florida grand jury secrecy law barred a witness from *ever* disclosing his testimony, even after the conclusion of the grand jury, it violated the First Amendment. 494 U.S. 624 (1990).

When government access to certain information held by a third party is authorized by statute, Congress has, in some instances, created a notice prohibition for grand jury subpoenas. For example, the Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3422, which ordinarily requires the financial institution to notify the customer where the government has subpoenaed the customer's records, provides for a "grand jury subpoena" exception under which banks are barred from notifying their customers of a grand jury subpoena either when the government obtains a court order delaying notification under Section 3409(a) or where the records are sought to investigate crimes against a financial institution or supervisory agency under Section 3420(b).

Other statutes permit the disclosure of information held by a third party to a law enforcement authority pursuant to a grand jury subpoena, but do not specify whether the affected consumer should be or can be notified of the existence or content of the subpoena. *See, e.g.*, 15 U.S.C. § 168(b) (consumer credit reports). The lack of a notification requirement for grand jury subpoenas has been a topic of scholarly work advocating for the extension of the American Bar Association's Criminal Justice Standard on Law Enforcement Access to Third Party Records to grand jury subpoenas. *See* Andrew E. Tazlitz and Stephen E. Henderson, *Reforming the Grand Jury to Protect Privacy in Third Party Records*, 64 American Univ. L. Rev. 195 (2014).

If they exist, notice requirements for an *administrative* subpoena served on a third party (issued at the discretion of the empowered agency without court review) are found in individual statutes. Because records held by a third party are usually governed by the third-party doctrine, and therefore Fourth Amendment protections do not extend to them, *see United States v. Miller,* 425 U.S. 435 (1976), an individual generally may not claim a right to notice of a subpoena served on a third party unless it is afforded by a specific statute. *See, e.g.*, *SEC v. Jerry T. O'Brien, Inc.* 467 U.S. 735, 742-43 (1984) (finding that the Securities Act of 1933 did not require notice of a subpoena to a target of an SEC investigation, and concluding that the SEC was not required to give notice to the target where administration of such notice would be highly burdensome or "increase the ability of persons who have something to hide to impede legitimate investigations").

Unlike grand jury subpoenas, however, there is no general expectation of secrecy for administrative subpoenas, and it is unclear whether a third-party recipient is forbidden from disclosing the existence and content of a subpoena to the target of an investigation.

One statute, which authorizes administrative subpoenas in several federal crimes, including health care offenses, child exploitation, and threats to Secret Service protectees, permits the government to seek ex parte gag orders under specified circumstances such as when notice risks "endangerment to the life or physical safety of any person," "flight to avoid prosecution," "destruction of or tampering with evidence," or the "intimidation of potential witnesses." 18 U.S.C. § 3486(a)(6)(B); *id.* § 3486(a)(6)(A) ("A United States district court for the district in which the summons is or will be served, upon application of the United States, may issue an ex parte order that no person or entity disclose to any other person or entity . . . the existence of such summons for a period of up to 90 days."); *id.* § 3486(a)(6)(C) ("An order under this paragraph may be renewed for additional periods of up to 90 days upon a showing that the circumstances described in subparagraph (b) continues to exist.").

b. Notice in the Digital World

The SCA and the PRA expressly provide for no notice or delayed notice for all warrants, court orders, and subpoenas authorized by those laws, and different notice requirements apply depending on which provision is in use.

One of the key issues in the digital context is that, even when there may be a Fourth Amendment notice requirement, that requirement may be satisfied by giving a copy of the warrant and receipt to the *third-party provider* under Rule 41(f)(1)(C).

This means that if the provider does not want to notify the affected member of the news media, or cannot because the provider is subject to a Section 2705(b) gag order, the affected member of the news media could conceivably never find out that the communications and attendant metadata have been seized. This is effectively what happened in the Rosen case. *See In re Application of the United States*, 665 F. Supp. 2d 1210 (D. Or. 2009) (finding that even if the notice requirement in Rule 41(f)(1)(C) applies to SCA warrants, it is satisfied by leaving the warrant and a receipt for the property seized with the third-party ISP).

i. Seizure of Electronic Communications Under the SCA

The SCA warrant provisions are complex and a relic of early email, in which storage was at a premium and it was rare for users to leave messages in electronic storage either with their internet provider or even on their computer. Typically, users would download a message from their provider and print out a physical copy. (Indeed, some early email providers would actually print email messages and send them by physical mail to the user.)

Accordingly, the law makes a distinction between newer and older emails, and between emails that are opened (and therefore assumed abandoned if left on a server) or unread. Put simply, for emails that are unopened and have been on the provider's server for 180 days or fewer, law enforcement must secure a warrant under 18 U.S.C. § 2703(a).

For emails that are older than 180 days or opened, law enforcement can use a warrant "without required notice to the subscriber" under 18 U.S.C. § 2703(b)(1)(A). With prior notice, which, as discussed below can be delayed indefinitely, the SCA permits authorities to compel the production of older or opened email, or other electronic communications content, with a Section 2703(d) order, or even a bare trial, grand jury, or administrative subpoena.

Under current practice, however, the Justice Department will use a full SCA warrant to demand any communications content. This follows a Sixth Circuit case that expressly held that emails receive full Fourth Amendment protection and therefore ordinarily cannot be seized without a probable cause warrant. *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). Accordingly, the government will argue that there is no notification requirement to the subscriber per Section 2703(a)-(b) or, as several courts have found, any notice requirement under Rule 41 is satisfied by leaving the warrant with the third-party communications provider.

With respect to the Section 2705 gag, Section 2705(b) then permits a government entity to effectively secure a prohibition on the *third-party provider* notifying the subscriber. If the court determines that there is reason to believe that notification of the existence of the warrant would have an adverse result (again endangering life or physical safety, flight from prosecution, destruction of or tampering with evidence, intimidation of potential witnesses, or otherwise

seriously jeopardizing or unduly delaying a trial), it "shall" enter the order "for such period as the court deems appropriate." Section 2705(b).[6]

In April 2016, Microsoft sued to challenge the constitutionality of these gags under the First and Fourth Amendments. In the suit, it noted that in the previous 18 months before filing, it had received 5,600 demands for data, of which 2,600 came with Section 2705(b) gag orders, including 1,750 with no fixed end date. *See* Ellen Nakashima, *Justice Department Moves to End Routine Gag Orders on Tech Firms*, Wash. Post, Oct. 24, 2017, https://perma.cc/8REP-C6QU.

Microsoft dropped the suit after the Justice Department issued binding guidance – subject to change at the discretion of the department – that purports to limit the use and duration of Section 2705(b) gags. *See* Policy Regarding Applications for Protective Orders Pursuant to 18 U.S.C. § 2705(b) at 2 (Oct. 19, 2017), https://assets.documentcloud.org/documents/4116326/Protective-Orders.pdf.

Under the new procedures:

- Prosecutors may only seek gags for up to a year "barring exceptional circumstances." *Id.* at 2;
- The policy specifically identifies certain national security investigations as being of the type that may justify a longer gag. *Id.* at 2 n.2;
- Nothing in the policy bars an indefinite gag;
- Prosecutors must conduct an "individualized and meaningful" assessment regarding the necessity of a gag. *Id.* at 2; and
- Any gag must be tailored to the particular adverse result contemplated. *Id.*

In sum, there is a distinct scenario where a member of the news media is subject to an SCA warrant and will never learn about it. That is, where any notice requirement under Rule 41 is satisfied by serving the warrant on the third-party provider, and where the provider is either unwilling to notify the subscriber or where it is unable to do so because of an indefinite Section 2705(b) notice preclusion order.

---

[6] There is some confusion under the plain terms of Section 2705(b) as to whether it even applies to either Section 2703(a) (permitting seizure of electronic communications in electronic storage for fewer than 180 days) or Section 2703(c) (permitting the seizure of various types of non-content information). Some courts, however, adopt a "holistic" approach that permits the issuance of a Section 2705(b) gag for all SCA investigative tools, regardless of which subsection they are authorized under. *See In re Application of the United States*, 131 F. Supp. 3d 1266, 1272 (D. Utah 2015) (finding that Section 2705 gag orders available for non-content demands under Section 2703(c) and that logic of holding would permit same for Section 2703(a) warrants). Note that regardless of whether a Section 2705 gag order is available, the delayed notice provision for warrants, Section 3103a, would likely apply.

ii. Section 2703(d) Orders and Subpoenas

For non-content records sought using a (d) order or subpoena, the analysis is, in comparison with SCA warrants for communications content, relatively simple. Section 2703(c) permits the government to demand non-content communications records using various tools. There is no notice requirement on the government at all, Section 2703(c)(3), and the government can preclude notification from the third-party provider using a potentially indefinite Section 2705(b) gag order.

Using an administrative, grand jury, or trial subpoena, the government can compel the production of basic subscriber information from a third-party electronic communications provider, including subscriber names, addresses, local and long-distance connection records, session time and duration records, length and types of service, telephone or instrument number, subscriber identifier (including any temporarily assigned network address), and payment information. 18 U.S.C. § 2703(c)(2).

Other types of non-content records – such as email or text transactional logs – can be obtained with a Section 2703(d) court order, which requires a showing of "specific and articulable facts" that the records are "relevant and material" to a criminal investigation. So-called (d) orders can reach a large number and array of sensitive transactional records held by third-party electronic communications providers. For instance, until the Supreme Court's recent decision in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), law enforcement used (d) orders to obtain cell-site location information, and may have done so to seize records pertaining to Ali Watkins in the James Wolfe case.

Again, under Section 2703(c)(3) there is no notification requirement at all and, despite some confusion over the phrasing of Section 2705(b), the "holistic view" adopted by the district court in Utah and asserted by the Justice Department (see footnote 5, above) is that an indefinite gag can be obtained to forever bar the third-party provider from notifying the subscriber that her records had been seized. *See In re Application of the United States*, 131 F. Supp. 3d 1266, 1272 (D. Utah 2015) (finding that Section 2705 gag orders available for non-content demands under Section 2703(c)).

Absent the 90-day provision in the Section 50.10 guidelines, non-content demands using (d) orders or subpoenas, coupled with a Section 2705(b) gag, could keep an affected news organization from ever finding out about the seizure of its communications or business records.

iii. PR-TT

The PRA has a separate indefinite notice preclusion provision for PR-TT orders. Under 18 U.S.C. § 3123(d), the order authorizing the use of a PR-TT device shall direct 1) that the order be sealed until otherwise ordered by the court and 2) that the recipient of the order be gagged from disclosing its existence "unless or until otherwise ordered by the court."

c. The James Rosen Case

The James Rosen case merits further discussion, as the government sought to keep the existence of a Gmail warrant secret from Rosen and Fox News for an extended period of time, and potentially in perpetuity (partly because it wanted to repeatedly search the account over time). Rosen did not find out about the search warrant until he read about it in the Washington Post, three years after his Gmail account had been searched. Ryan Lizza, *How Prosecutors Fought to Keep Rosen's Warrant Secret*, New Yorker (May 24, 2013), https://perma.cc/973J-Q8ZK.

In the Rosen case, the government applied for an SCA warrant for Rosen's account on May 28, 2010. *See* Mem. and Order, *In re Application for Warrant for Email Account [Redacted]@gmail.com*, Mag. No. 10-291-M-01 (AK/JMF/RCL) (D.D.C. Nov. 1, 2010). Magistrate Judge Alan Kay checked the box on the warrant for a "sneak and peek" search, but the government, believing it had no obligation to notify Rosen at all, had not requested a "sneak and peek" warrant, which, they believed, would have required notice on some date certain. *Id*. at 1.

Accordingly, the government filed a "motion for clarification" of the magistrate judge's checking of the box. Former Magistrate Judge John M. Facciola for the U.S. District Court for the District of Columbia handled the motion and found that the government had an obligation to notify Rosen of the warrant. He rejected the government's reasoning that the plain language of the SCA precludes a notification requirement. *See id.*

The government had, prior to the Facciola order, contacted Judge Kay, who returned the original warrant with a notation that he had checked the "sneak and peek" box in error. *See id.* 2 n.1. The government asserted that Kay had thus adjudicated the motion for clarification. Facciola, however, contacted Kay, who confirmed that he believed that the revised order meant that the Justice Department would notify Rosen without delay. *Id.*

The case ended up before Judge Lamberth, who found that the notice provision in Rule 41, by its plain terms, only required that the warrant and receipt be left with the third-party ISP. *Id.* at 7. Because Google was subject to a section 2705(b) gag, which did not include an expiration date, the Rosen search warrant presents arguably the worst-case scenario: where notice of an email seizure to the owner of the emails is precluded forever, and the email provider is powerless to notify the customer.

Interestingly, another development in the Rosen case illustrates in stark terms the severity of this result (and the perversity of having the guidelines only apply to telephone toll subpoenas). In addition to a search warrant, the Justice Department used a subpoena to compel the production of toll records for over 30 telephone numbers, including five numbers belonging to Fox News. Ryan Lizza wrote about the subpoenas in 2013, and the Justice Department announced at the time that it *had* notified News Corp., Fox News's parent company at the time, of the subpoenas because of the guidelines.[7]

[7] There is some confusion over whether News Corp. was indeed notified and whether it told Fox News. Following the Lizza story, News Corp. acknowledged receipt of the notice, but its former general

In other words, prior to the 2014-2015 revisions in the guidelines to include search warrants, the Justice Department would have been able to forever keep secret that it had seized a reporter's email, but it had to notify the outlet that the reporter's comparatively less sensitive phone records had been seized.

Importantly, were the Justice Department to seek a warrant similar to the Rosen Gmail warrant under the current guidelines, the result should be different on several fronts.

Notably, the Justice Department would not be able to use the "suspect exception" in the Privacy Protection Act, 42 U.S.C. § 2000aa(a)(1), as the "offense" would have arisen out of newsgathering activity and the purpose of the search warrant was solely to further the investigation of the source, not the member of the news media. 28 C.F.R. § 50.10(d)(4)-(5). To delay notice of the warrant, to the extent the warrant would even be available, the attorney general would have to make an affirmative showing of an adverse result.

In short, under the current guidelines, it's not even clear that notice of the Rosen warrant could be delayed at all, and notice would, in any event, be required within 90 days. The Rosen case is therefore a potent example of the check provided by the hard 90-day backstop in the revised guidelines and a strong argument for its retention.

IV. Conclusion

As described above, the 90-day backstop in the Section 50.10 guidelines may be, in several contexts, the only way that an affected member of the news media could receive notice that her communications or records had been seized and scrutinized as part of a criminal investigation. Indeed, the 90-day backstop is an unusual notice provision in that it does not permit indefinite extensions of notice, which is a particularly valuable protection for the press.

This backstop can be justified under the theory that, while members of the news media should be treated unexceptionally when they are under investigation for crimes not arising out of newsgathering, when prosecutors pursue their communications and business records as part of investigating other matters, source and work product protections mandate that they be given the ability to challenge overbroad or inappropriate process before it issues.

When extraordinary circumstances permit, delay may be warranted, but it is equally important that the member of the news media be guaranteed that they will eventually – and in the near term – learn of the seizure of their records or communications.

Were the backstop removed, whether at 90 days or some other time certain, the only "guarantee" of notice would be if the relevant records or communications were publicly used in a criminal proceeding, or if the affected member of the news media were to bring a constitutional challenge to an indefinite delay of notice. In order to bring such a challenge, the affected member of the

---

counsel, who would have personally received the notice, disputed that account. *See* Ryan Lizza, *News Corp. vs. Fox News*, New Yorker (May 27, 2013), https://perma.cc/P36H-DBTE.

news media would have to know about the government demand, which, as a practical matter, limits potential recourse.

If the Justice Department were not merely to extend the backstop for additional 45-day terms but to remove it entirely, it might incentivize prosecutors to more frequently find that the presumption in favor of notice that appears in Section 50.10(e)(2) (and elsewhere) in the guidelines does not apply. After all, under the current rules, when the department determines that the presumption in favor of notice has been overcome, it still knows that the day of reckoning is ahead, either 45 days after the return or perhaps 90. But if there is no hard backstop under Section 50.10, there may be no day of reckoning placed on the Justice Department by rules outside of the guidelines, as this memorandum demonstrates.

Finally, notice provides benefits to the Justice Department as well. The two times that the guidelines have been substantively revised – first in 1980 and then in 2014-2015 – were the result of the Justice Department correcting course after widely-publicized overreaching against the press. Were prosecutors to remove this key restraint from the guidelines, they would lose the check that only routine transparency can provide and invite louder public outcry at some future time when any investigative excesses involving reporters (inevitably) come to light.

Default Notice Requirements Without News Media Guidelines 90-Day Backstop

Type	Materials Searched or Seized	Tool	Delay	Gag
Physical	Tangible things or a search without seizure.	Rule 41 search warrant; Rule 41(f)(1)(C) requires officer to leave warrant and, if items are seized, a receipt with the person searched or whose premises the property was taken, or at the premises searched.	Sneak and peek warrants authorized under 18 U.S.C. § 3103a; delay for 30 days or longer if facts justify; may extend on good cause shown; indefinite extensions.	Prosecutors have applied for a gag on the third-party recipient in certain cases (unclear how common).
	Third-party records (bank, credit card, health, student, etc.).	Grand jury, administrative, or trial subpoenas.	Authorized by individual statutes but many with no notice requirement.	Statute specific; 18 U.S.C. § 3486, for instance, authorizes gag for 90 days, with indefinite 90-day extensions available upon showing of need.
Electronic	Content (emails, texts, voicemails).	SCA search warrant (post-*Warshak* federal authorities use warrants for all content).	Courts often permit no-notice, reasoning that Rule 41 notice requirement, to the extent it applies, is satisfied by delivery of copy to provider.	Gag authorized under 18 U.S.C. § 2705(b) "for such period as the court deems appropriate."
	Transactional records (e.g., email logs, some location information).	Court order under § 2703(d) (a "(d)" order).	No notice required under § 2703(c)(3).	Gag authorized under 18 U.S.C. § 2705(b) "for such period as the court deems appropriate."
	Basic subscriber information.	Trial, grand jury, or administrative subpoena.	No notice required under § 2703(c)(3).	Gag authorized under 18 U.S.C. § 2705(b) "for such period as the court deems appropriate."
	Prospective phone and email metadata collection.	PR-TT order.	Orders are, by default, sealed under 18 U.S.C. § 3123(d)(1).	Recipient of order shall not disclose existence of order "unless or until otherwise ordered by the court." § 3123(d)(2).