

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION**

| | | |
|-------------------------|---|--------------------------|
| IN RE SEALING AND | § | |
| NON-DISCLOSURE OF | § | MAGISTRATE NO. H-08-218M |
| PEN/TRAP/2703(d) ORDERS | § | MAGISTRATE NO. H-08-219M |
| | § | |

MEMORANDUM AND ORDER

Cell phones and e-mail play just as big a role in criminal investigations as they do in everyday life. Two federal statutes¹ authorize law enforcement to compel telephone companies and Internet service providers to allow real-time monitoring of customer telephone and Internet usage (non-content), and to turn over customer phone records, cell site locations, stored e-mails, and other account information. Both statutes require a court order authorizing these forms of electronic surveillance in the course of a criminal investigation.

This opinion addresses a recurring issue of electronic surveillance law not previously decided in a published case: whether these electronic surveillance court orders may properly be kept secret, by sealing and non-disclosure provisions, for an indefinite period beyond the underlying criminal investigation.

On March 19, 2008, the Government submitted two applications for a pen register and trap/trace device on two cell phones allegedly used by an individual engaged in illegal drug

¹ These statutes, known as the Pen/Trap Statute and the Stored Communications Act (“SCA”), were enacted in 1986 as separate parts of the Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986). They are codified at 18 U.S.C. §§ 3121-27 and 18 U.S.C. §§ 2701-12, respectively.

trafficking. Following its usual practice in this district, the Government combined each application with a request for customer information regarding the target phones under SCA § 2703(d). Each application concluded with the Government's standard request that the combined pen/trap/2703(d) orders (and underlying applications) be sealed and not disclosed by the service provider to the user or subscriber "until further order of the court." This court has acceded to such requests in the past, but almost never has occasion to revisit them, as shown below. The result has been a kudzu of sealed manila envelopes overflowing the clerk's office vault.

Upon further deliberation, the court is convinced that setting a fixed expiration date on sealing and non-disclosure of electronic surveillance orders² is not merely better practice, but required by law: in particular, the First Amendment prohibition against prior restraint of speech and the common law right of public access to judicial records. The considerations underlying this departure from previous practice are explained below.

Background

To appreciate the extent of the problem, it is necessary to understand how this segment of the criminal docket works. Magistrate judges in this district handle a significant volume of pretrial criminal proceedings, including initial appearances, appointment of counsel, arraignments, detention hearings, preliminary hearings, criminal complaints, grand

² As used in this opinion, the phrase "electronic surveillance orders" refers to pen register and trap/trace orders, § 2703(d) orders for stored e-mail, telephone records, and customer account information, cell site location orders, and tracking device warrants. Wiretap orders are not included.

jury returns, and arrest warrants. This criminal docket also includes *ex parte* investigative matters prior to indictment or complaint, including search warrants, seizure warrants, and electronic surveillance orders. To keep track of these *ex parte* orders, a supplemental docket system known as the “Green Book” was developed. The Green Book is an oversized, cloth-bound volume containing handwritten entries by the case manager for the duty magistrate judge. A separate Green Book is issued each year. Each entry is docketed under a separate “M” case number, and under that number are typically filed the Government’s application, affidavits, and other supporting material, as well as any orders of the court, including extensions and sealing orders. Sealed orders are maintained in sealed manila envelopes marked “Sealed by Order of Court.” With the advent of CM/ECF,³ Green Book entries are transferred to the publicly-accessible electronic docket. Sealed cases are designated on CM/ECF only by case number and type of case, *e.g.*, “H-08-218M Pen Register.”

Based on publicly available CM/ECF data, court staff conducted a survey of electronic surveillance orders issued by magistrate judges in the Southern District of Texas, Houston Division, for the period 1995-2007. The results, compiled in Table A (attached), reveal that 3877 out of 4234 electronic surveillance orders issued during this period, 91.6%, remain completely sealed. Almost all of these orders provide that they are sealed “until further order of the court.” Moreover, the vast majority of the 357 unsealed orders were not sealed initially; only 9 currently accessible orders had been previously sealed. This means that out

³ CM/ECF refers to the court’s “Case Management/Electronic Case Filing” system, which allows remote electronic access to the court’s docket.

of 3886 orders sealed “until further order of the court,” 99.7% remain under seal today, many years after issuance. These numbers confirm, beyond reasonable doubt, that when it comes to shielding electronic surveillance orders from the public, indefinitely sealed means permanently sealed.

Relevant Statutes

Any evaluation of sealing and non-disclosure orders must begin with the governing statutory scheme.

The Pen/Trap Statute (18 U.S.C. §§ 3121-27). This statute, which authorizes electronic surveillance in the form of pen registers and trap/trace devices, specifically addresses both the sealing and non-disclosure of pen/trap orders. Section 3123(d)(1) of Title 18 directs that pen/trap orders be sealed “until otherwise ordered by the court.” No particular showing is required to justify sealing; nor is there any suggested sealing period, although it is fair to presume that sealing should last at least as long as the surveillance authorized by the order itself – 60 days.⁴ How long a pen/trap order should be sealed, and whether sealing should continue beyond the life of the pen register itself, is left to the sound discretion of the court.

⁴ 18 U.S.C. § 3123(c)(1). Extensions of up to 60 days can be granted upon re-application to the court. *Id.* at § 3123(c)(2).

The statute also addresses non-disclosure, sometimes colloquially referred to as a “gag order.”⁵ Section 3123(d)(2) provides that the “the person owning or leasing the line or other facility to which the pen register or a trap and trace device is attached, or applied, or who is obligated by the order to provide assistance to the applicant” shall be directed not to disclose to any other person the existence of the pen/trap or the investigation “unless or until otherwise ordered by the court.” Again, no particular showing by the government is required to justify non-disclosure, and no minimum time period is imposed or even suggested. In fact, the “unless” clause implies that the court may refuse to enjoin disclosure even in the first instance. In the end, the duration of any gag order remains subject to the court’s discretion.

Stored Communications Act (18 U.S.C. §§ 2701-12). The SCA is different. Nothing in that statute mentions sealing of orders granting access to telephone and e-mail subscriber information. The SCA does allow for “preclusion of notice” to any other person of the existence of the order, but only if there is reason to believe that notification will result in—

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

18 U.S.C. § 2705(b)(1)-(5).⁶

⁵ See *United States v. Brown*, 218 F.3d 415 (5th Cir. 2000).

⁶ The SCA also allows up to 90 days delayed notice of § 2703(b) orders granting access to certain stored e-mail, upon a showing that notice may trigger the same “adverse results” listed in 18 U.S.C. § 2705(a). These provisions, currently the subject of *en banc* proceedings (continued...)

Precluding the service provider from giving notice of a § 2703(d) order is certainly a type of gag order, although the prohibited act is “notice” rather than “disclosure.” Whether such a notice preclusion order would also prohibit a truthful response to an unsolicited customer inquiry is debatable. In any event, the duration of notice preclusion under § 2705(b) is “for such period as the court deems appropriate,” so again, the duration of this limited gag order is at the discretion of the issuing judge.⁷

⁶ (...continued)
in the Sixth Circuit, were previously ruled unconstitutional by a panel of that court. *See Warshak v. United States*, 490 F.3d 455 (6th Cir.), *vacated upon grant of rehearing en banc*, No. 06-4092, 2007 U.S. App. LEXIS 23741 (6th Cir. Oct. 9, 2007). The deferred notice provisions of the SCA are not at issue here, although the five adverse results justifying delayed notice under § 2705(a) are identical to those justifying preclusion of notice under § 2705(b). The only apparent difference is that the § 2705(a) standard for delaying notice (“may have an adverse result”) is more lenient than the § 2705(b) standard for precluding notice (“will result in”adverse result).

⁷ The Government’s practice in this district of combining pen/trap applications with requests for customer information under § 2703(d) has the advantage of efficiency, but at the cost of added legal uncertainty. Neither the Pen/Trap Statute nor the SCA expressly contemplates such a combination, so it is unclear which statute is controlling. With regard to sealing, this uncertainty is of little consequence. Although the Pen/Trap Statute requires sealing and the SCA does not, nothing in the SCA limits the court’s discretion to seal 2703(d) orders. The statutes are materially different regarding notice, however. The SCA authorizes a limited gag order only where there is reason to believe notification “will result in” a specified adverse consequence. The Pen/Trap Statute imposes no such threshold condition, and so would allow a gag order in circumstances where the SCA would not. In order to avoid such a legally dubious end-run around the SCA’s threshold for gag-orders, it will be assumed that the non-disclosure of combined pen/trap/2703(d) orders is governed by the more restrictive SCA.

Analysis

1. The First Amendment and Non-Disclosure Orders

The practice of issuing secret electronic surveillance orders without an expiration date raises troubling legal questions too often avoided. The task is complicated by the fact that the sealing and non-disclosure provisions are subject to different legal standards. Even though each provision contributes to the order's concealment from the general public, gag orders implicate somewhat different interests than sealing orders. Judicial gag orders impinge upon freedom of speech and press under the First Amendment, and must pass muster under well-established constitutional case law. On the other hand, sealed judicial orders conflict with the common law tradition of public access to judicial proceedings, and are typically evaluated under more flexible common law rules. This section will focus upon gag orders and the First Amendment.

The constitutionality of an indefinite § 2703(d) non-disclosure order has not been specifically addressed in any published decision. However, the Fifth Circuit has acknowledged in an unpublished opinion that “substantial constitutional questions [are] raised by a nondisclosure order without any limitation as to time.” *United States v. ApolloMedia Corp.*, No. 99-20849, 2000 WL 34524449, *3 (5th Cir. June 2, 2000).⁸

⁸ The *ApolloMedia* court did not decide the issue, but remanded for reconsideration in light of changed circumstances on appeal. *ApolloMedia*, an Internet service provider, had received a § 2703(d) order compelling production of information concerning a customer suspected of sending threatening e-mails. *ApolloMedia*, seeking to publicize the government's investigation on its website, appealed the indefinite gag order on First
(continued...)

At the outset, it is appropriate to acknowledge that First Amendment rights are not absolute and do not automatically override all other constitutional values in case of conflict. *See Nebraska Press Ass'n v. Stuart*, 427 U.S. 539, 570 (1976) (“We reaffirm that the guarantees of freedom of expression are not an absolute prohibition under all circumstances, but the barriers to prior restraint remain high and the presumption against its use continues intact.”). Government-imposed limitations on freedom of speech are subject to greater or lesser degrees of scrutiny depending upon contextual factors such as the type of speech involved, the severity of the regulation, *etc.* The most searching form of scrutiny, called “strict scrutiny,” is reserved for the protection of speech implicating the core concerns of the First Amendment. *Republican Party of Minn. v. White*, 536 U.S. 765, 774-75 (2002).

Regulation of speech. The non-disclosure rule at issue here limits speech. The recipient of the order — that is, “the person owning or leasing the line or other facility to which the pen register or trap and trace device is attached, or applied, or who is obligated by the order to provide assistance to the applicant” — is forbidden from disclosing to anyone the

⁸ (...continued)

Amendment grounds. The investigation was discontinued while the appeal was pending, so the district court modified its order to allow ApolloMedia to disclose the existence of the investigation and the sealed order, but continued to restrain ApolloMedia from revealing specific identifying information regarding the victim and the alleged crime. At oral argument, the government conceded that disclosure of the redacted information would not compromise the investigation, but asserted that the gag order was justified by its policy of not disclosing the names of victims “at any time, even when the crime is never prosecuted.” Noting that the underlying statute authorized non-disclosure only upon a showing of certain specified harms, the court elected to remand the case for determination whether that portion of the non-disclosure order should remain in effect.

existence of either the pen/trap device or the underlying investigation. Such a “naked prohibition against disclosure is fairly characterized as a regulation of pure speech.” *Bartnicki v. Vopper*, 532 U.S. 514, 526 (2001) (referring to analogous Wiretap Act provision prohibiting disclosure of contents of illegally intercepted communication). Nor does it matter that the “person” restrained from speaking may be a corporate entity such as a telecommunications company. *See First Nat’l Bank of Boston v. Bellotti*, 435 U.S. 765, 777 (1978) (“The inherent worth of the speech in terms of its capacity for informing the public does not depend upon the identity of its source, whether corporation, association, union, or individual.”). The question thus becomes, what degree of constitutional scrutiny should be applied to this restriction of speech?

Content-based. A regulation that merely limits the time, place, or manner of speech is constitutionally permissible if it serves a significant governmental interest and leaves ample alternative channels for communication. *See Cox v. New Hampshire*, 312 U.S. 569 (1941).

But a valid time-place-manner restriction “may not be based upon either the content or subject matter of speech.” *Consol. Edison Co. of New York v. Pub. Serv. Comm’n*, 447 U.S. 530, 536 (1980). One form of content-based regulation is a law that distinguishes favored speech from disfavored speech on the basis of the ideas or views expressed. *See Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 643 (1994). Another is a law that closes off a particular subject matter from public discourse. *Consol. Edison*, 447 U.S. at 537 (“The First

Amendment’s hostility to content-based regulation extends not only to restrictions on particular viewpoints, but also to prohibition of public discussion of an entire topic.”).

The gag orders in question are content-based because they effectively preclude speech on an entire topic — the electronic surveillance order and its underlying criminal investigation. Prohibiting a service provider from disclosing the existence of the pen/trap or the investigation means that the first-hand experiences of the recipients of these orders are completely excluded from the public debate. *See Doe v. Gonzales*, 500 F. Supp. 2d 379, 396-97 (S.D.N.Y. 2007) (holding that non-disclosure restrictions upon national security letter recipients are content-based). Of course, the burden of the gag order probably falls more heavily upon the target of the surveillance rather than the service provider, whose business interests are arguably unaffected by non-disclosure.⁹ While it may be true that, even without a gag order, the telecommunications company would not be particularly inclined to notify its customer of ongoing electronic surveillance, it is also irrelevant. If the recipients of pen/trap orders are forever enjoined from discussing them, the individual targets may never learn that they had been subjected to such surveillance, and this lack of information will inevitably stifle public debate about the proper scope and extent of this important law enforcement tool.¹⁰ By

⁹ *But see ApolloMedia Corp.*, 2000 U.S.App. LEXIS 38754 (Internet service provider challenged gag order preventing communication to its customers regarding circumstances giving rise to § 2703(d) order).

¹⁰ *See Paul Schwartz, Reviving Telecommunications Surveillance Law*, 75 U. CHI. L. REV. 287, 287 (2008) (contending that rational inquiry about telecommunications surveillance has been “largely precluded by the haphazard and incomplete information the government collects (continued...)”).

constricting the flow of information at its source, the government dries up the marketplace of ideas just as effectively as a customer-targeted injunction would do. Given the public's intense interest in this area of law, such content-based restrictions are subject to rigorous scrutiny. *See generally Sheppard v. Maxwell*, 384 U.S. 333 (1966); *United States v. Brown*, 250 F.3d 907, 915 (5th Cir. 2001).

Prior restraint. Besides restricting content, a non-disclosure order imposes a prior restraint on speech. The First Amendment provides greater protection from prior restraints than from subsequent punishments. *Alexander v. United States*, 509 U.S. 544, 554 (1993).¹¹ Prior restraints “are constitutionally disfavored in this nation nearly to the point of extinction.” *Brown*, 250 F.3d at 915.

The Supreme Court has declared that “[any] system of prior restraints of expression comes to this Court bearing a heavy presumption against its constitutional validity,” and that the Government “carries a heavy burden of showing justification for the imposition of such a restraint.” *Capital Cities Media, Inc. v. Toole*, 463 U.S. 1303, 1305 (1983) (citation omitted). In order to justify such a prior restraint, the government must demonstrate that (1) the activity restrained poses a clear and present danger or a serious and imminent threat to a

¹⁰ (...continued)
about it”). The prevalence of non-disclosure orders may partly explain the relatively small number of reported decisions in this area of law.

¹¹ In the words of one authoritative commentator, “Prior restraints fall on speech with a brutality and a finality all their own. . . . A criminal statute chills, prior restraint freezes.” ALEXANDER M. BICKEL, *THE MORALITY OF CONSENT* 61 (Yale University Press, 1975).

compelling government interest; (2) less restrictive means to protect that interest are unavailable; and (3) the restraint is narrowly-tailored to achieve its legitimate goal. *Brown*, 250 F.3d at 915-18; *see generally Nebraska Press Ass'n v. Stuart*, 427 U.S. 539 (1976).

A prior restraint has traditionally been defined as a “predetermined judicial prohibition restraining specified expression.” *Bernard v. Gulf Oil Co.*, 619 F.2d 459, 467 (5th Cir. 1980) (*en banc*), citing *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539, 559 (1976). The distinguishing features of a prior restraint are (1) its judicial origin, although an enabling statute may authorize the order which “places specific communications under the personal censorship of the judge;” (2) the purpose is suppression rather than punishment; (3) the means of enforcement is the contempt power of the court, which is “more swiftly imposed and less subject to the mitigating safeguards of the criminal justice system;” and (4) the inability to assert constitutional invalidity as a defense in contempt proceedings. *Bernard* at 468-69. Each of these tell-tale markers of prior restraint is readily exhibited by the non-disclosure orders at issue here.

Countervailing interests. In correspondence with this court, the Government has asserted two interests in support of this prior restraint: (1) the integrity of the investigation and (2) the reputational interests of innocent targets. The integrity interest is already reflected in SCA § 2705(b), which lists the various ways in which an ongoing investigation might be jeopardized by disclosure: endangering the life or physical safety of an individual, flight from prosecution, destruction or tampering with evidence, intimidation of potential witnesses, and

undue trial delay. As the Supreme Court has recognized, however, the government's legitimate interest in the integrity of its investigation does not automatically trump First Amendment rights. For example, in *Landmark Communications, Inc. v. Virginia*, 435 U.S. 829 (1978), a newspaper publisher was convicted under a Virginia statute making it a crime to divulge information about proceedings pending before the state judicial review commission. The Supreme Court overturned the conviction on First Amendment grounds. While assuming that confidentiality of judicial review proceedings served legitimate state interests, the Court held those interests insufficient to justify the encroachment on freedom to speak about a core First Amendment topic such as possible misconduct by the state judiciary. The Court concluded that the state had "offered little more than assertion and conjecture to support its claim that without criminal sanctions the objectives of the statutory scheme would be seriously undermined." *Id.* at 841.

Even more salient is *Butterworth v. Smith*, 494 U.S. 624 (1990), where the Court held that a Florida grand jury statute violated the First Amendment insofar as it prohibited a grand jury witness from disclosing his own testimony *after* the grand jury investigation ended. Acknowledging the state's interests in preserving grand jury secrecy as outlined in *Douglas Oil Co. of California v. Petrol Stops Nw.*,¹² the Court found these interests either inapplicable

¹² 441 U.S. 211 (1979). Grand jury secrecy (1) encourages witnesses to come forward; (2) minimizes witness tampering; (3) minimizes risk of flight by targets of investigation; (4) reduces undue influence upon grand jurors; and (5) protects reputation of persons accused but exonerated. *Id.* at 218-19.

or insufficient to sustain the permanent ban on a witness's disclosure of his own testimony once the grand jury has been discharged:

When an investigation ends, there is no longer a need to keep information from the targeted individual in order to prevent his escape — that individual will presumably have been exonerated, on the one hand, or arrested or otherwise informed of the charges against him, on the other. There is also no longer a need to prevent the importuning of grand jurors since their deliberations will be over. Similarly, the concern that some witnesses will be deterred from presenting testimony due to fears of retribution is, we think, not advanced by this prohibition; any witness is free *not* to divulge his own testimony . . .

494 U.S. at 632-33 (footnote omitted). The ban's effectiveness in preventing subornation of grand jury witnesses was also deemed "marginal at best and insufficient to outweigh the First Amendment interest in speech involved." *Id.* at 634.

Butterworth also rejected as inadequate the government's second compelling interest asserted here, *i.e.*, that persons accused but exonerated by the grand jury should not be held up to public ridicule.¹³ The Court conceded that such a ban might protect a target's reputation in some cases, but noted that it might have the opposite effect when a target desires to "go public" and exonerate himself by publishing his own grand jury testimony. In any case, "our decisions establish that absent exceptional circumstances, reputational interests alone cannot justify the proscription of truthful speech." *Butterworth*, 494 U.S. at 634.¹⁴ The Court

¹³ See also *Bartnicki v. Vopper*, 532 U.S. 514, 534 (2001) ("[P]rivacy concerns give way when balanced against the interest in publishing matters of public importance.").

¹⁴ Citing *Landmark*, 435 U.S. at 841-42 ("injury to official reputation is an insufficient reason for repressing speech that would otherwise be free"); *Florida Star v. B.J.F.*, 491 U.S. 524 (1989) (First Amendment precluded State from imposing damages for publication of rape (continued...))

bolstered its holding by noting that the drafters of the Federal Rules of Criminal Procedure had found it unnecessary to impose any obligation of secrecy on grand jury witnesses in order to protect reputational or other legitimate interests.¹⁵ The *Butterworth* opinion concludes by emphasizing the unacceptable burden entailed by Florida's prohibition on a witness's ability to make a truthful public statement:

The ban extends not merely to the life of the grand jury but *into the indefinite future*. The potential for abuse of the Florida prohibition, through its employment as a *device to silence those who know of unlawful conduct or irregularities on the part of public officials*, is apparent.

494 U.S. at 635-36 (emphasis added).

Butterworth's concerns about indefinite bans of silence are no less applicable here. The basic context is the same: a witness in possession of information material to a criminal investigation is barred from making public statements about a matter of public interest for an indefinite period of time after the investigation is closed. It is true that not every criminal investigation generates the same degree of public interest as a probe of alleged impropriety by government officials, as in *Butterworth* or *Landmark Communications*. In fact the underlying investigation here does not involve public corruption charges. But that does not

¹⁴ (...continued)
victim's name); *Smith v. Daily Mail Publishing Co.*, 443 U.S. 97 (1979) (State could not constitutionally punish the publication of a juvenile offender's name); *Oklahoma Publishing Co. v. Oklahoma County Dist. Court*, 430 U.S. 308 (1977) (State could not constitutionally enjoin the publication of juvenile offender's name).

¹⁵ See FED. R. CRIM. P. 6(e)(2), which expressly prohibits certain individuals other than witnesses from disclosing "a matter occurring before the grand jury," and provides that "[n]o obligation of secrecy may be imposed on any person except in accordance with [this rule]."

mean that investigative techniques routinely employed by law enforcement are unworthy of public scrutiny and debate. To the contrary, the use of new and innovative technology to investigate, apprehend, and prosecute criminal suspects is a regular staple of media attention at local, state, and national levels.¹⁶ Nor is public concern about law enforcement techniques a recent phenomenon.¹⁷ E-mail and cell phones may not have been part of eighteenth century life, but the framers were acutely concerned about the proper limits upon government intrusion into citizens' lives.¹⁸

It is appropriate here to address another interest not asserted in the government's correspondence, but included in the government's application to this court: "[T]he exact nature of the United States 'pen register' device and its configuration is classified as a law enforcement sensitive investigative technique, the disclosure of which would likely jeopardize other on-going investigations, and/or future use of the technique." In certain contexts, a qualified "law enforcement privilege" to protect government files related to an ongoing investigation has been recognized by a majority of circuits, including the Fifth Circuit. *See*

¹⁶ *See, e.g.*, Matt Richtel, *Live Tracking of Mobile Phones Prompts Court Fights on Privacy*, N.Y. Times, Dec. 10, 2005, §A at 1; Jonathan Krim, *FBI Dealt Setback on Cellular Surveillance*, Wash. Post, Oct. 28, 2005; Ellen Nakashima, *Cell Phone Tracking Lacks Limits*, Houston Chronicle, Nov. 23, 2007, §A, at 1; Larry Copeland, *Red Light Cameras Work: They're Changing Behavior, But Some Say Rights Violated*, USA Today, Feb. 15, 2007.

¹⁷ *See, e.g.*, *Olmstead v. United States*, 277 U.S. 438 (1928) (wire-tapping).

¹⁸ *See United States v. United States Dist. Court*, 407 U.S. 297, 317 (1972) ("The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech.").

generally In re U.S. Dep't of Homeland Sec., 459 F.3d 565 (5th Cir. 2006); 26A CHARLES ALAN WRIGHT & KENNETH W. GRAHAM JR., FEDERAL PRACTICE & PROCEDURE § 5681 (1992). However, no published Fifth Circuit decision has extended this privilege to require sealing of court records beyond an ongoing investigation. Nor has this court found any federal case extending the privilege to pen registers in general. There are many good reasons why this court should not be the first to break such new ground.

First of all, pen register configuration is not “classified information” in the strict national security sense. Classified information is governed by the Classified Information Procedures Act, and its definition of the term does not encompass pen/trap devices used for ordinary criminal law enforcement.¹⁹ Second, neither the order nor the application would disclose the “exact nature or configuration” of the device. Even if they did, the reader would find nothing more informative than what could easily be found on the Internet, including the

¹⁹ 18 U.S.C. app. 3 § 1(a) defines “classified information” as “information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security and any restricted data, as defined in paragraph r. of section 11 of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)).”

Supreme Court's own website.²⁰ In other words, that horse has long since left the barn, gone for a gallop down the information superhighway.

Finally, the argument that disclosure of this "sensitive" investigative technique would somehow jeopardize other investigations, now or in the future, simply proves too much. Muzzling telecoms to prevent disclosure of pen/trap orders might in the odd case deprive a fugitive of useful information, but it would also deprive the law-abiding public of significant data about the frequency of compelled Government access to individual e-mail and phone records. If that sort of trade-off were legally acceptable, then the Government would be free to cloak in secrecy *any* investigative technique, from the most mundane search warrant to the most sophisticated electronic surveillance, thereby avoiding the disinfecting rays of public scrutiny. That result might seem felicitous to zealous and well-meaning officers of the law, but it misconceives the indispensable role of daylight in our system of justice:

[E]specially in the administration of criminal justice, the means used to achieve justice must have the support derived from public acceptance of both the process and its results. . . . People in an open society do not demand infallibility from their institutions, but it is difficult for them to accept what they are prohibited from observing

Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 571-72 (1980).

²⁰ See, e.g., *Kyllo v. United States*, 533 U.S. 27, 29-30 (2001) (describing in detail how a thermal-imaging device is used to detect indoor marijuana growth); *Bartnicki v. Vopper*, 532 U.S. 514, 523 n. 6 (2001) (noting that techniques and devices for intercepting cell and cordless phone calls can be found in various publications, trade magazines, and Internet sites); *United States v. New York Tel. Co.*, 434 U.S. 159, 160-62 (1977) (describing in detail the installation and operation of a pen register used to investigate illegal gambling); see also *United States Telecom Ass'n v. Federal Communications Comm'n*, 227 F.3d 450 (D.C. Cir. 2000) (describing in detail new telecommunications technology designed to assist law enforcement under the Communications Assistance for Law Enforcement Act of 1994).

The potential for abuse of the witness gag order cited in *Butterworth* — that it would be employed “as a device to silence those who know of unlawful conduct or irregularities on the part of public officials”²¹ — is likewise present here. And the potentially pernicious effects of concealing even lawful conduct should not be overlooked. Cumulatively considered, these secret orders, issued by the thousands year after year by court after court around the country, may conceal from the public the actual degree of government intrusion that current legislation authorizes. It may very well be that, given full disclosure of the frequency and extent of these orders, the people and their elected representatives would heartily approve without a second thought. But then again, they might not.

Conclusion. An indefinite non-disclosure order is tantamount to a permanent injunction of prior restraint. To the extent such an order enjoins speech beyond the life of the underlying investigation, it must be narrowly tailored to serve a compelling governmental interest in order to pass muster under the First Amendment. The governmental interests considered here — the integrity of an ongoing criminal investigation, the reputational interests of targets, and the sensitivity of investigative techniques — are not sufficiently compelling to justify a permanent gag order. And because the statutes authorizing these non-disclosure orders must be construed whenever possible in a manner that avoids constitutional infirmity,²²

²¹ 494 U.S. at 635-36.

²² See; *Clark v. Martinez*, 543 U.S. 371, 381 (2005) (as between “competing plausible interpretations of a statutory text,” Congress most likely “did not intend the alternative which raises serious constitutional doubts.”); *Hooper v. California*, 155 U.S. 648, 657 (1895) (continued...)

it follows that neither 18 U.S.C. § 2705(b) nor § 3123(d) may be interpreted to permit a gag order of indefinite duration.

This does not preclude the possibility that in a particular case the government may be able to demonstrate that a particular order or portion thereof should not be disclosed when the investigation ends. For example, the Government may be able to establish that the life or physical safety of an individual will continue to be endangered after the investigation is closed.²³ Of course, the narrow-tailoring requirement entails that redaction of objectionable information should be considered as an alternative before tossing a blanket of silence over the entire order. In any event, electronic surveillance gag orders of unlimited duration must be the exception rather than the rule.

2. The Common Law Right of Public Access and Sealed Judicial Orders

The sealing of judicial records imposes a limit on public access rather than a direct restriction on speech. Even so, the Supreme Court has recognized a First Amendment right of public access to criminal trials, including certain pretrial proceedings. *See Richmond Newspapers, Inc.*, 448 U.S. at 580 (press and public have a First Amendment right of attend a criminal trial); *Globe Newspaper Co. v. Superior Court*, 457 U.S. 596 (1982) (First Amendment right of access to a minor victim's testimony in a rape trial); *Press-Enterprise Co.*

²² (...continued)
("Every reasonable construction must be resorted to, in order to save a statute from unconstitutionality.").

²³ *See* 18 U.S.C. § 2705(b)(1).

v. Superior Court, 464 U.S. 501 (1984) (*Press-Enterprise I*) (public right to attend jury selection); *Press-Enterprise Co. v. Superior Court*, 478 U.S. 1 (1986) (*Press-Enterprise II*) (right of access to preliminary hearing and transcript). No court has yet considered whether electronic surveillance orders fall within the ambit of the First Amendment's right of public access.

The public's right of access to judicial records has long been acknowledged at common law, however. *See Nixon v. Warner Communications, Inc.*, 435 U.S. 589, 597 (1978). Because constitutional adjudication is inevitably hazardous, especially when so few lampposts are in sight, sealing orders are typically evaluated under common law standards. In a similar case involving a newspaper's claimed right of access to a search warrant affidavit containing wiretap information, Judge Alvin Rubin wrote: "To determine whether there is such a right, we first look to the common law, for we need not, and should not, reach the First Amendment issue if judgment can be rendered on some other basis." *In re Application of Newsday, Inc.*, 895 F.2d 74, 78 (2d Cir. 1990) (Rubin, J., sitting by designation). That prudent advice will be followed here.

Historical background. "What transpires in the court room is public property." *Craig v. Harney*, 331 U.S. 367, 374 (1947). "[J]ustice cannot survive behind walls of silence" *Sheppard v. Maxwell*, 384 U.S. 333, 349 (1966). "[S]ecret judicial proceedings would be a menace to liberty." *Gannett Co. v. DePasquale*, 443 U.S. 368, 412 (1979) (Blackmun, J. concurring and dissenting). These truisms are founded upon centuries of unbroken legal

history. Indeed, the tradition of publicity is one of the most ancient features of our common law system, predating not only the constitution but also the Magna Carta itself. *See Richmond Newspapers Inc.*, 448 U.S. at 564-65 (tracing the history of public trials in the days before the Norman Conquest); *see also Gannett Co.*, 443 U.S. at 419-27 (Blackmun, J., concurring and dissenting) (“[T]he common law from its inception was wedded to the Anglo-Saxon tradition of publicity . . .”). Interestingly, this tradition of publicity existed even before the Norman kings introduced the jury system to English law.²⁴

Authoritative sources on English common law agree that publicity was an inseparable concomitant of English justice.²⁵ As royal courts took over the administration of justice, the public nature of the proceedings became intrinsically associated with its public setting. Coke explained that the very words “*In curia Domini Regis*” in the Statute of Marlborough of 1267 meant that court proceedings would be public:

These words are of great importance, for all Causes ought to be heard, ordered, and determined before the Judges of the King’s Courts openly in the King’s Courts, whither all persons may resort; and in no chambers, or other private places: for the *Judges are not Judges of chambers, but of Courts*, and therefore in open Court, where the parties Council and Attorneys attend, ought orders,

²⁴ Anglo-Saxon criminal trials “were by compurgation or by ordeal and took place invariably before the assembled community, many of whom were required to attend.” *Gannett Co.*, 443 U.S. at 419 (Blackmun, J., concurring and dissenting).

²⁵ 1 WILLIAM SEARLE HOLDSWORTH, *A HISTORY OF ENGLISH LAW* 7-24, 316 (Methuen & Co. 1927) (1903); FREDERICK POLLOCK, *THE EXPANSION OF THE COMMON LAW* 3132 (Stevens and Sons 1904); MATTHEW HALE, *THE HISTORY OF THE COMMON LAW OF ENGLAND*, 343, 345 (H. Butterworth 1820); 3 WILLIAM BLACKSTONE, *COMMENTARIES* 372 (W. Maxwell 1855).

rules, awards, and judgments to be made and given, and not in chambers or other private places. . .

2 EDWARD COKE, INSTITUTES OF THE LAWS OF ENGLAND 103 (Rawlins 1680) (emphasis added).²⁶

The English common law view of a court as a public forum was transplanted to colonial America. The first public trial provision to appear in America emphasized the public's right to attend both civil and criminal trials:

That in all publick courts of justice for tryals of causes, civil or criminal, any person or persons, inhabitants of the said Province may freely come into, and attend the said courts, and hear and be present, at all or any such tryals as shall be there had or passed, that *justice may not be done in a corner nor in any covert manner.*

THE CONCESSIONS AND AGREEMENTS OF THE PROPRIETORS, FREEHOLDERS, AND INHABITANTS OF THE PROVINCE OF WEST NEW JERSEY IN AMERICA (1677), ch. xxiii, *quoted in* 1 BERNARD SCHWARTZ, THE BILL OF RIGHTS: A DOCUMENTARY HISTORY 129 (Chelsea House Publishers 1971) (emphasis added).

Out of this common law tradition grew the explicit Sixth Amendment guarantee of an open criminal trial, as well as the implicit First Amendment right of the public and press to attend criminal trials and related proceedings. *Richmond Newspapers, Inc.*, 448 U.S. at 580-81. “[T]he historical evidence demonstrates conclusively that at the time our organic laws

²⁶ The conception of a court as a public place to conduct public business can be traced to ancient Athens. One of the reforms attributed to Pericles was the establishment of popular courts called *heliatae*, so named because the sessions were held in the open air under the sun (*helios*). WILL DURANT, THE STORY OF CIVILIZATION: THE LIFE OF GREECE 259 (Simon and Schuster 1939).

were adopted, criminal trials both here and in England had long been presumptively open. This is no quirk of history; rather, it has long been recognized as an indispensable attribute of an Anglo-American trial.” *Id.* at 584. In fact, part of the test required to establish a constitutional right of access to a judicial proceeding is a showing that “the place and process have historically been open to the press and general public.” *Press-Enterprise II*, 478 U.S. at 8-9. As Justice Brennan noted in his *Richmond Newspapers* concurrence, this tradition of accessibility commands respect because it carries “the favorable judgment of experience.” 448 U.S. at 589.

Richmond Newspapers describes several vital functions that publicity performs in our judicial system. First, it discourages misconduct among the trial participants and improves the quality of testimony.²⁷ Second, publicity acts as a check on the potential abuse of judicial power.²⁸ Finally, and perhaps most important, it has the “significant community therapeutic value” of promoting public confidence in the judicial system. *Id.* at 556. “Even without such experts to frame the concept in words, people sensed from experience and observation that,

²⁷ 6 JOHN HENRY WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW § 1834 (Aspen Publishers 2006).

²⁸ The Court invokes the famous dictum of Jeremy Bentham: “Without publicity, all other checks are insufficient: in comparison of publicity, all other checks are of small account.” 1 JEREMY BENTHAM, RATIONALE OF JUDICIAL EVIDENCE SPECIALLY APPLIED TO ENGLISH PRACTICE 524 (Hunt and Clark 1827). Other philosophers past and present might also be cited. *See, e.g.*, IMMANUEL KANT, PERPETUAL PEACE 47 (Liberal Arts Press 1957) (“Every legal claim must be capable of publicity. . . . [W]ithout it there can be no justice (which can only be conceived as publicly known) and thus no right, since it can be conferred only in accordance with justice.”); JOHN RAWLS, A THEORY OF JUSTICE 175-82 (Belknap Press of the Harvard University Press 1971) (publicity is necessary condition for a stable conception of justice).

especially in the administration of criminal justice, the means used to achieve justice must have the support derived from public acceptance of both the process and its results.” *Id.* at 570-71.

Judicial records. *Richmond Newspapers* was decided in the context of a First Amendment right to attend a criminal trial, but the valuable functions attributed to publicity apply not only to the actual proceedings but also to the records of those proceedings.²⁹ The first Supreme Court case to acknowledge the common law right of public access involved judicial records. *Nixon*, 435 U.S. at 597.

Nixon involved a dispute over copies of presidential tape recordings that had been introduced at a criminal trial. The trial court had denied permission for television networks to copy the tapes for commercial distribution. While affirming the trial court’s decision, the Supreme Court recognized the common law right of access to judicial records based on interests as fundamental as “the citizen’s desire to keep a watchful eye on the workings of public agencies, and . . . a newspaper publisher’s intention to publish information concerning the operation of government.” *Id.* at 598. The right is not absolute, of course, and the trial court must exercise sound discretion in weighing the countervailing factors. *Id.* at 599. The *Nixon* Court found it unnecessary “to delineate precisely the contours of the common law

²⁹ See, e.g., *United States v. Ochoa-Vasquez*, 428 F.3d 1015, 1029-30 (11th Cir. 2005) (recognizing First Amendment right to access court docket sheets); *Hartford Courant v. Pellegrino*, 380 F.3d 83, 93-94 (2d Cir. 2004) (same); *United States v. Valenti*, 987 F.2d 708, 715 (11th Cir. 1993) (same). See generally Hannah Levine, *Toward a New Public Access Doctrine*, 27 *Cardozo L. Rev.* 1739 (2006); Meliah Thomas, *Commentary The First Amendment Right of Access to Docket Sheets*, 94 *Cal. L. Rev.* 1537 (2006).

right,” because the records there in dispute were available for public access under terms prescribed by Congress in the Presidential Recordings Act.³⁰ *Id.* In light of that statutory “decisive element,” the trial court was found to have properly exercised its discretion in refusing to authorize release of the Nixon tapes for commercial distribution.

Before delving into post-*Nixon* cases on the common law right of access, it is critical to identify the type of “judicial record” at issue. The universe of judicial records may be envisioned as a three-drawer filing cabinet. In the bottom drawer are the bulk of unfiled documents and information generated by the discovery process. As a general rule, documents not yet admitted or filed with the court do not become available to the public simply because they have been produced in the judicially-managed discovery process. *See Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 33 (1984) (“pretrial depositions and interrogatories are not public components of a civil trial . . . [and] were not open to the public at common law”). Such materials, though subject to the judicial process, should probably not be considered judicial records at all. *See e.g., SEC v. Van Waeyenberghe*, 990 F.2d 845, 849 (5th Cir. 1993) (“Once a settlement is filed in district court, it becomes a judicial record”); *Baxter Int’l Inc. v. Abbott Labs*, 297 F.3d 544, 545 (7th Cir. 2002) (“Secrecy is fine at the discovery stage, before the material enters the judicial record.”).

The middle drawer consists of pleadings, documents, affidavits, exhibits, and other materials filed by a party or admitted into evidence by the court. Such documents are

³⁰ 44 U.S.C. § 2101 *et seq.*

presumptively open for public inspection and copying, although various federal rules permit such documents to be filed in redacted form, under seal, or both.³¹ Not all filed documents have equal public interest, however. Dispositive documents, that is documents that influence or underpin the judicial decision, are “open to public inspection unless they meet the definition of trade secrets or other categories of bona fide long-term confidentiality.” *Baxter*, 297 F.3d at 545. Such documents may not be shielded from public view by mere agreement of the parties. “[M]any litigants would like to keep confidential the salary they make, the injuries they suffered, or the price they agreed to pay under a contract, but when these things are vital to claims made in litigation they must be revealed.” *Id.* at 547. Most litigation over the common law right of access appears to involve this middle drawer of judicial records.

In the top drawer of judicial records are documents authored or generated by the court itself in discharging its public duties, including opinions, orders, judgments, docket sheets, and other information related to the court’s public functions. Unlike the lower two, this drawer is hardly ever closed to the public. Federal statutes³² and rules³³ confirm the important

³¹ Federal Rule of Civil Procedure 5.2 authorizes the court to order that a filing be made under seal, or that certain information be redacted for “good cause.” Under Rule 26(c), a party may move for an order requiring the sealing of depositions or other filings upon a showing of good cause. *See In re Equal Employment Opportunity Comm’n*, 709 F.2d 392, 402 n.7 (5th Cir. 1983) (ruling that testimonial and investigatory interests were inadequate to justify sealing informant’s affidavit in EEOC subpoena enforcement action).

³² For example, the E-Government Act of 2002 was intended to promote governmental use of the Internet and emerging technologies “to provide citizen-centric [*sic*] Government information and services,” and thereby “make the Federal Government more transparent and accountable.” Pub. L. 107-347, 116 Stat. 2899 (Dec. 17, 2002), *codified at* 44 U.S.C.A. § 3601, note. Section 205(a) of the Act requires federal courts to maintain websites providing (continued...)

distinction, for purposes of public access, between judicial rulings and other case-related filings. The rationale for heightened public access to this sort of judicial record was cogently put by Judge Easterbrook when confronted with sealed lower court opinions in a recent trade secret case:

What happens in the federal courts is presumptively open to public scrutiny. Judges deliberate in private but issue public decisions after public arguments based on public records. The political branches of government claim legitimacy by election, judges by reason. **Any step that withdraws an element of the judicial process from public view makes the ensuing decision look more like fiat and requires rigorous justification.** The Supreme Court issues public opinions in all cases, even those said to involve state secrets. *See New York Times Co. v. United States*, 403 U.S. 713 (1971). A district court issued public opinions in a case dealing with construction plans for hydrogen bombs. *United States v. Progressive, Inc.*, 467 F. Supp.990, *rehearing denied*, 486 F. Supp. 5 (W.D. Wis.), *appeal dismissed*, 610 F.2d 819 (7th Cir. 1979). We issued a public opinion in a case whose subject was attorney-client confidences that required the parties' names and many details to be withheld. *See A Sealed Case*, 890 F.2d 15 (7th Cir. 1989). It is impossible to see any justification for issuing off-the-record opinions in a dispute about drawings of transmission testing equipment. . . The Clerk of this court will place the district court's opinions in the public record. **We hope never to encounter another sealed opinion.**

³² (...continued)

on-line access to “docket information for each case” as well as “the substance of all written opinions issued by the court, regardless of whether such opinions are to be published in the official court reporter, in a text searchable format.” The possibility of sealing such court documents is not mentioned, in pointed contrast to the section (§ 205(c)) on “electronic filings,” which does recognize that “documents filed under seal” will not be made available online. In other words, sealing of court opinions is too rare to be mentioned, while sealing of filed documents is common enough to be addressed.

³³ *See e.g.* FED. R.CIV. P. 5.2, which restricts electronic access to case files in Social Security and immigration proceedings, except that the public is entitled to full remote electronic access to “(A) the docket maintained by the court; and (B) an opinion, order, judgment, or other disposition of the court, but not any other part of the case file or administrative record.”

Hicklin Eng'g, L.C. v. Bartell, 439 F.3d 346, 348-49 (7th Cir. 2006) (emphasis added).³⁴

With this three-drawer cabinet in mind, the court now turns to the Government's request to seal these electronic surveillance orders beyond the life of the underlying investigation. This sealing request involves "top drawer" judicial records, because it encompasses everything in the court file, including the orders themselves.

Search warrant case law. While no case directly on point has been found, perhaps the most analogous³⁵ cases are those dealing with sealed search warrants. Three circuits have ruled that there is at least a common law right of public access to a search warrant application once the warrant had been executed and filed with the clerk. *See In re Application of Newsday, Inc.*, 895 F.2d 74, 79 (2d Cir.) (Rubin, J., sitting by designation); *Baltimore Sun Co. v. Goetz*, 886 F.2d 60, 64-65 (4th Cir. 1989); *In re Search Warrant for Secretarial Area Outside the Office of Thomas Gunn*, 855 F.2d 569, 573 (8th Cir.1988) (holding that the right to inspect search warrant materials arises under both common law and the First Amendment). One circuit has held that there was no constitutional or common law right to inspect a warrant application

³⁴ Of course, Congress has occasionally passed legislation mandating secrecy of judicial rulings in certain sensitive areas. *See* Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.*; False Claims Act, 31 U.S.C. § 3730; 18 U.S.C. § 5038 (limiting disclosure of records of juvenile delinquency proceedings). By contrast, in the context of electronic surveillance Congress has chosen to rely upon judicial discretion, as noted previously.

³⁵ Grand jury no-bill decisions, which are normally kept from the public, are fundamentally different. Unlike electronic surveillance orders, a no-bill does not affirmatively authorize government coercion affecting property rights or other interests of a citizen. Moreover, as the Supreme Court in *Butterworth* noted, the limits of grand jury secrecy are specified by rule. 494 U.S. at 634-35. There are no such rules for electronic surveillance orders; the governing statutes leave the matter to the court's discretion.

“during the pre-indictment stage of an ongoing criminal investigation.” *Times Mirror Co. v. United States*, 873 F.2d 1210, 1221 (9th Cir. 1989). No Fifth Circuit decision reaches the issue, although one Texas district court followed the Ninth Circuit in declining public access to such materials while the investigation was ongoing. *In re Search Warrants in connection with Investigation of Columbia/HCA Healthcare Corp.*, 971 F. Supp. 251 (W.D. Tex. 1997). The three circuit decisions granting public access relied heavily upon the provision of Rule 41 (now Rule 41(i)) directing the judicial officer to file all papers relating to the search warrant in the clerk’s office. *See, e.g., In re Application of Newsday, Inc.*, 895 F.2d at 79 (“[T]here is a common law right to inspect what is commanded thus to be filed.”).

In summary, no court has ruled that search warrant applications may be sealed indefinitely after the investigation comes to a close. On the contrary, sealing of search warrant affidavits is “an extraordinary action” to be taken only in exceptional cases. *See* WRIGHT, KING & KLEIN, FEDERAL PRACTICE AND PROCEDURE, CRIMINAL 3d § 673, at 332-33 (2004).³⁶

Fifth Circuit authority. The Fifth Circuit has recognized the district court’s authority to seal the record of judicial proceedings, but cautions that such discretion “is to be exercised charily.” *FSLIC v. Blain*, 808 F.2d 395, 399 (5th Cir.1987) (upholding lower court decision to unseal an agreed injunction after one party breached the seal). Most of its cases do not deal with top drawer court-generated records. *See ACLU v. Mississippi*, 911 F.2d 1066 (5th Cir.

³⁶ The practice in this division was consistent with this rule until recent years. Review of the Houston Division criminal docket shows that for the years 1995-2001 between 13% and 25% of search warrants were issued under seal. Since 2002, the range has risen to between 52% and 72%. No explanation for this sea change is apparent on the face of the docket.

1990) (state commission files containing sensitive personal information); *In re Equal Employment Opportunity Comm'n*, 709 F.2d 392, 401 n.7 (5th Cir. 1983) (sealed affidavits in EEOC subpoena enforcement action); *Belo Broad. Corp. v. Clark*, 654 F.2d 423 (5th Cir. 1981) (copies of audiotapes introduced as evidence in public official bribery trial).

However, on at least two occasions the Fifth Circuit has considered the sealing of district court orders and reversed the lower court in each instance. In *Van Waeyenberghe*, the parties had agreed on a consent decree and final order of permanent injunction in a case involving violations of federal securities laws. 990 F.2d at 847. At the insistence of the individual defendant (Schwartz), and over the government's objection, the trial court ordered that the permanent injunction and the transcript of proceedings be sealed. On appeal, the Fifth Circuit held that the common law presumption of public access to judicial records was applicable to settlement agreements filed and submitted to the district court for approval. Although the weight to be given the presumption was not specified, a trial court must balance the public's right of access against the interests favoring secrecy. *Id.* at 848. Here the trial court had erroneously assumed that the public's interest in knowing about Schwartz's injunction could best be served by requiring Schwartz himself to make that disclosure before engaging in future transactions. As the court explained:

Although the public may have a right to the *information* that Schwartz was enjoined, that right cannot be equated with the public's right of access to *judicial records*. The public's right to information does not protect the same interests that the right of access is designed to protect. 'Public access [to judicial records] serves to promote trustworthiness of the judicial process, to curb judicial abuses,

and to provide the public with a more complete understanding of the judicial system, including a better perception of its fairness.’

Id. at 849 (emphasis in original) (quoting *Littlejohn v. BIC Corp.*, 851 F.2d 673, 682 (3d Cir. 1988)).

Most recently, the Fifth Circuit invoked basic judicial standards of transparency and fairness to disapprove indefinite sealing orders in a dispute over attorneys fees. *In re High Sulfur Content Gasoline Prods. Liab. Litig.*, 517 F.3d 220 (5th Cir. 2008). A class action settlement had set aside a lump sum fee award of \$6.9 million to be allocated among more than six dozen plaintiffs’ lawyers. The district court deferred the allocation decision to a fee committee headed by lead counsel for the plaintiffs, who submitted a proposed allocation of fees and costs at an *ex parte* hearing without notice to the affected attorneys. Upon accepting the committee’s proposed allocation, the court promptly sealed the fee allocation order, the hearing transcript, and even the docket minute entry for the hearing, all topped off with a gag order upon the plaintiffs’ attorneys.

Finding that the trial court abused its discretion by rubber-stamping the committee’s recommendation in this manner, the court declared:

The court made matters worse when it sealed the exhibit listing the individual fees and the record entries pertaining to fees and placed a gag order on the plaintiffs’ attorneys. These actions not only kept the public in the dark about each plaintiffs’ attorney’s award but also prevented counsel from communicating with each other and their own clients on the subject. The lack of transparency about the individual fee awards supports a perception that many of these attorneys were more interested in accommodating themselves than the people they represent.

Id. at 229. A district court has discretion to seal a record, but that discretion must be mindful of “the public nature of our judicial proceedings” and “the public’s right to be informed.” *Id.* at 230. The court reasoned that fee disputes, like other civil litigation, ought to be litigated openly:

Attorneys’ fees, after all, are not state secrets that will jeopardize national security if they are released to the public. . . . From the perspective of class welfare, publicizing the process leading to attorneys’ fee allocation may discourage favoritism and unsavory dealings among attorneys even as it enables the court to better conduct oversight of the fees.

Id. The court then quoted with approval a Third Circuit decision overturning a trial court’s denial of public access to criminal pretrial hearings:

Public confidence cannot long be maintained where important judicial decisions are made behind closed doors and then announced in conclusive terms to the public, with the record supporting the court’s decision sealed from public view.

United States v. Cianfrani, 573 F.2d 835, 851 (3d Cir. 1978).

High Sulfur thus echoes, in a civil context, the same justifications underlying the common law tradition of open court proceedings articulated in *Richmond Newspapers*: (1) to discourage misconduct among litigants; (2) to check potential abuse of judicial power; and (3) to promote public confidence in the judicial system. 448 U.S. at 569-73. If anything, those functions are more critical in the context of criminal proceedings, closely hedged as they are with constitutional constraints. It is doubtful that public interest in a prosecutor’s access to citizen phone records and e-mails is any less pervasive or intense than public curiosity about how a large group of plaintiffs’ lawyers splits up a fee award. Nor is it plausible that the

judicial record for allocating attorneys fees in a private dispute should be more transparent than the judicial record for setting in motion the formidable law enforcement machinery of the federal government. In short, *High Sulfur*'s standard of judicial transparency is no less applicable to electronic surveillance orders than to attorneys' fee awards.

Admittedly, *High Sulfur* did not involve the need to preserve the integrity of an ongoing criminal investigation. Because that legitimate interest will inevitably be present whenever an electronic surveillance order is issued, a temporary sealing order of some duration will almost always be necessary.³⁷ But as a general rule the need for sealing will last only so long as the underlying investigation is active.

Conclusion. Based on the foregoing authority, the court concludes that there is a common law right of public access to electronic surveillance orders at the post-investigation stage. This right is not absolute, and may be curtailed when sealing is (a) essential to preserve higher values and (b) narrowly tailored to preserve that interest, after consideration of less restrictive alternatives. *Baltimore Sun Co.*, 886 F.2d at 65-66; *In re Knight Publishing Co.*, 743 F.2d 231, 235 (4th Cir. 1984). Redaction is among the less restrictive alternatives that must be considered. It is difficult to conceive any circumstance under which permanent sealing of the entire file, including the order itself, could ever be justified. After all, top secret

³⁷ Pre-indictment access to such orders might be justified under appropriate circumstances. See, e.g., *In re Search Warrants Issued on April 26, 2004*, 353 F. Supp. 2d 584, 591 (D. Md. 2004) (affirming magistrate judge's order recognizing "a search subject's pre-indictment Fourth Amendment right to inspect the probable cause affidavit").

national security information is routinely de-classified after a number of years.³⁸ Legitimate confidentiality interests will almost always be fully accommodated by redacting the troublesome words or passages. *See Hicklin Eng'g*, 439 F.3d at 348-49.

Summary

These considerations lead, by slightly different paths, to the same end. As a rule, sealing and non-disclosure of electronic surveillance orders must be neither permanent nor, what amounts to the same thing, indefinite. Such restrictions on speech and public access are presumptively justified while the investigation is ongoing, but that justification has an expiration date. Publicity will not threaten the integrity of a criminal investigation that is no longer active. Once that point is reached, the fundamental values of openness and transparency embodied in the First Amendment and at common law must be given sway. We are judges of courts, not of chambers, and justice may not be done in a corner.

The remaining task is to fix a standard period for sealing and non-disclosure orders. Obviously, it is not possible to predict in advance how long a criminal investigation will take. The standard duration for a pen/trap order is 60 days,³⁹ but extensions are not uncommon. Given that time frame, a 180 day period seems most reasonable as a default setting for sealing and non-disclosure — short enough to respect the fundamental values at stake, and long enough not to cause an undue burden.


³⁸ 22 C.F.R. § 94(d) (2007).

³⁹ 18 U.S.C. § 3123(c).

Turning to the orders in this case, the sealing and non-disclosure provisions will expire on September 15, 2008, which is 180 days after they were entered. After that six month period, the orders will be unsealed and disclosable unless the Government moves to extend the ban for another 180 days based on (a) a certification that the investigation is still active, or (b) a showing of exceptional circumstances, *e.g.*, danger to the life or physical safety of an individual. For purposes of certification, a currently inactive or dormant investigation will not qualify for extension based on the mere possibility of reactivation at a later date. Additional extensions will be considered, but a correspondingly greater specificity in the certification will be required for each such extension. The Government will be given 30 days advance notice before the gag orders are lifted and unsealed.

This protocol for sealing and non-disclosure of electronic surveillance orders will be followed by this magistrate judge until further notice. Although the 180-day sealing and non-disclosure period represents a departure from previous practice, the change should bring no undue hardship. If experience proves otherwise, the court will revisit the issue and entertain any reasonable modifications the Government or other interested parties might wish to propose.

Signed at Houston, Texas on May 30, 2008.



Stephen Wm Smith
United States Magistrate Judge

TABLE A
Sealing of Electronic Surveillance Orders
1995-2007

| YEAR | # Issued | # Initially Sealed | # Unsealed | # Currently Sealed | % Currently Sealed |
|--------|----------|--------------------|------------|--------------------|--------------------|
| 1995 | 405 | 319 | 1 | 318 | 78.5 |
| 1996 | 378 | 301 | 0 | 301 | 79.6 |
| 1997 | 391 | 334 | 4 | 330 | 84.4 |
| 1998 | 390 | 380 | 1 | 379 | 97.1 |
| 1999 | 291 | 291 | 0 | 291 | 100 |
| 2000 | 286 | 276 | 1 | 275 | 96.0 |
| 2001 | 341 | 324 | 1 | 323 | 94.7 |
| 2002 | 277 | 228 | 0 | 228 | 82.3 |
| 2003 | 252 | 247 | 0 | 247 | 98.0 |
| 2004 | 326 | 324 | 1 | 323 | 99.1 |
| 2005 | 302 | 270 | 0 | 270 | 89.4 |
| 2006 | 251 | 248 | 0 | 248 | 98.8 |
| 2007 | 344 | 344 | 0 | 344 | 100 |
| TOTALS | 4234 | 3886 | 9 | 3877 | 91.6% |

Source: Docket records for the United States District Court, Southern District of Texas, Houston Division, as of April 1, 2008. “Electronic surveillance orders” include orders for pen registers, trap & trace devices, tracking devices, cell site location, stored email, telephone logs, and customer account records from electronic service providers. Wiretap orders are not included.