April 27, 2017

Hon. Janet C. Hall
Chief Judge
United States District Court for the
District of Connecticut
Richard C. Lee Courthouse
141 Church Street
New Haven, CT 06510

Re: Rules Governing Public Access to Search Warrant and Surveillance Material

Dear Chief Judge Hall:

We are writing to draw your attention to an issue of concern with the local rules and practices regarding the sealing of search warrants and electronic surveillance orders in the District of Connecticut. While this Court's rules mandate transparency for these court records to some extent, the rules currently allow for warrants and electronic surveillance orders to be sealed indefinitely. A study we pursued over the past six months revealed that these records typically do remain sealed in perpetuity, unless government attorneys seek to unseal specific items in the course of a prosecution.

This perpetual shroud of secrecy should not be acceptable. The systematic, permanent sealing of search warrants and electronic surveillance orders violates the public's right of access to judicial records; it prevents citizens from monitoring how prosecutors exercise their surveillance powers and from assessing how the judiciary balances the right of privacy against the needs of law enforcement. In the attached memorandum, we detail the findings from our investigation, review the public's common law and First Amendment rights to inspect these court records, and propose rules changes to address the deficiencies we found in current practices.

We urge you and the Rules Committee to consider the changes proposed, and we would be happy to discuss them with you at any time. Thank you in advance for your consideration of these important transparency issues.

Respectfully submitted,

Andrew Udelsman
*Law Student Intern*

Yurij Melnyk
*Law Student Intern*

cc: James T. Cowdery
Robin D. Tabora

MFIA MEDIA FREEDOM & INFORMATION ACCESS CLINIC

**M E M O R A N D U M**

TO: Hon. Janet C. Hall

CC: James T. Cowdery
Robin D. Tabora

FROM: Andrew Udelsman
Yurij Melnyk

DATE: April 27, 2017

RE: Rules Governing Public Access to Search Warrant and Surveillance Material[1]

## Introduction

> "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, 572 (1980).

The Fourth Amendment generally requires law enforcement officers to obtain search warrants before searching a suspect's physical property. Warrants are not required for certain forms of electronic surveillance—such as compelled disclosure of an individual's call records—but the statutes that authorize those types of surveillance require law enforcement officers to obtain court orders that function similarly to warrants. Search warrants and surveillance orders share the same purpose: they allow "an objective mind" to "weigh the need to invade [individuals'] privacy in order to enforce the law."[2]

Both search warrants and electronic surveillance orders are initially sealed as a matter of course, and for good reason. A "compelling need" for secrecy typically exists during an ongoing investigation. But once an investigation has concluded, the need for secrecy dissipates. Search warrants and surveillance orders should then become available for public inspection, with redactions if necessary, just like other court records.[3] Perpetual sealing of these materials

---

[1] This memorandum was prepared by students in the Media Freedom and Information Access Clinic, a program of the Abrams Institute for Freedom of Expression at Yale Law School. The memorandum does not purport to express the school's institutional views, if any.

[2] *See McDonald v. United States,* 335 U.S. 451, 455 (1948) (describing the purpose of search warrants).

[3] The Connecticut District already has rules detailing the types of personal identifying information that must be redacted from public filings. *See* Privacy Policy, United States District Court, District of Connecticut, Feb. 28, 2012, *http://www.ctd.uscourts.gov/sites/default/files/PRIVACY%20POLICY%202-28-12.pdf*.

violates a qualified right of public access to court records protected by both the common law and the First Amendment. Perpetual sealing allows an important government function to proceed entirely in secrecy, increasing the likelihood of arbitrary behavior and decreasing public confidence in "the conscientiousness, reasonableness, [and] honesty" of our law enforcement system.[4]

Unfortunately, perpetual sealing of search warrants appears to be the default norm in many federal courts;[5] in districts like Connecticut, warrants are typically unsealed only if they become relevant over the course of a specific prosecution. Practices surrounding electronic surveillance orders are even more troubling. The number of such sealed orders issued each year is massive: according to one estimate, in 2006 federal judges issued over 30,000 sealed orders authorizing electronic surveillance.[6] The number has almost certainly grown over the past decade, and in some districts that have been studied only 0.1 percent of such orders ever become public.[7] Some district courts—including Connecticut—do not even docket the fact that electronic surveillance has been authorized.

In an effort to ascertain the sealing and unsealing practices in this District, we have reviewed the rules of court, studied the public docket, and interviewed prosecutors and court personnel.[8] Our investigation revealed several areas where reform is needed to meaningfully protect the public's right of access and the important democratic interests served by openness. For example, we found that indefinite sealing has resulted in approximately 1/6 of all criminal cases docketed between January 1, 2000 and February 22, 2017 to be identified in ECF only as "Sealed v. Sealed." The majority of these "Sealed v. Sealed" cases apparently involve search warrant applications that did not become relevant in a prosecution, but that is impossible to confirm. Even more troubling is that orders authorizing electronic surveillance are not docketed at all in this District; the public has no way of ascertaining even *how many times* pen registers, trap and trace devices, or compelled disclosures of communications metadata have been authorized by the federal courts in Connecticut.

We describe below the deficiencies we identified in the current rules and practices in Connecticut and propose reforms to address them. Section I first describes the scope of the public's qualified common law and constitutional rights of access to judicial records, and Section II explains why those rights properly extend to search warrants, surveillance orders, and the supporting government affidavits. In Section III, we present our findings regarding current

---

[4] *See United States v. Amodeo*, 71 F.3d 1044, 1048 (2d Cir. 1995) ("*Amodeo II*").

[5] Stephen Smith, *Gagged, Sealed, and Delivered: Reforming ECPA's Secret Docket*, 6 HARV. LAW & POLICY REV. 313, 317 (2012).

[6] Smith, *supra* note 5 at 320-21.

[7] Spencer S. Hsu & Rachel Weiner, *U.S. Courts: Electronic Surveillance up 500 percent in D.C.-Area Since 2011*, WASH. POST (Oct. 24, 2016), http://wapo.st/21gRxeW.

[8] We extend our sincere gratitude to William J. Nardini, U.S. Attorney and Chief of the Criminal Division, David E. Novick, U.S. Attorney, and members of the District Court's Clerk's Office for sharing their time and insights with us.

sealing practices in Connecticut district courts, and Section IV provides recommendations for amendments to the local rules that will improve the public's access to important information it is entitled to know. Most importantly, we urge the Court to adopt a docketing system for sealed surveillance orders and to adopt a sunset provision for all sealing orders, so that search warrant and surveillance materials will automatically be unsealed by a date certain unless the United States Attorney's Office makes a showing that continued sealing is necessary in a specific case.

We urge you to review this issue and to adopt new rules that will end the permanent secrecy that currently deprives the public of important information about how invasive law enforcement tools are being used by prosecutors and the manner in which courts are enforcing constitutional privacy protections.

## I. The Common Law and the First Amendment Confer a Right of Public Access to Judicial Records.

Transparency plays a critical role in our democratic system. That system depends on citizens having access to information about how the government is functioning, so that they might evaluate the system's effectiveness and, when necessary, demand change. The Second Circuit has noted that transparency is particularly vital within the judicial branch:

> Although courts have a number of internal checks, such as appellate review by multi-judge tribunals, professional and public monitoring is an essential feature of democratic control. Monitoring both provides judges with critical views of their work and deters arbitrary judicial behavior. Without monitoring, moreover, the public could have no confidence in the conscientiousness, reasonableness, or honesty of judicial proceedings. Such monitoring is not possible without access to testimony and documents that are used in the performance of Article III functions.[9]

While in some cases concerns will be present that outweigh the benefits of transparency, there is a strong presumption that documents "used in the performance of Article III functions" will be available for public inspection. That presumption is grounded in the common law and the public's right of access is protected by the First Amendment.

*The common law right of access.*

The common law provides a qualified right "to inspect and copy public records and documents, including judicial records and documents."[10] This right predates the Constitution[11]

[9] *Amodeo II*, 71 F.3d at 1048.

[10] *Nixon v. Warner Commc'ns, Inc.*, 435 U.S. 589, 597 (1978) (footnote omitted); *see also In re Application of Newsday, Inc.*, 895 F.2d 74, 79 (2d Cir. 1990) ("[T]here is a common law right to inspect what is commanded thus to be filed.").

[11] *U.S. v. Amodeo*, 44 F.3d 141, 145 (2d Cir. 1995) ("*Amodeo I*").

and is intended to improve the accountability of federal courts, while increasing "confidence in the administration of justice."[12] The right attaches to "judicial records," defined by the Second Circuit Court of Appeals as documents filed with a court and "relevant to the performance of the judicial function and useful in the judicial process."[13]

The common law right of access creates a presumption of openness that varies in strength depending on the role the record in question plays "in the exercise of Article III judicial power."[14] After determining the strength of the presumption of access in an individual case, courts examine any "countervailing factors" that compete against openness.[15]

*The First Amendment right of access.*

The First Amendment conveys a distinct right of access to records relating to criminal proceedings. That qualified right derives from protection that the First Amendment provides for the "free discussion of governmental affairs."[16] Allowing public access to court documents ensures "that the individual citizen can effectively participate in and contribute to our republican system of self-government."[17]

The Supreme Court first articulated the scope of the First Amendment right in the context of public attendance at a criminal trial,[18] and subsequently applied the right to related criminal proceedings, including witness testimony,[19] the transcripts of *voir dire* proceedings,[20] and preliminary hearings.[21] The Second Circuit has recognized that the right extends to other judicial proceedings and records, including pre-trial motion papers,[22] videotape evidence,[23] suppression hearings,[24] and plea hearings.[25]

---

[12] *Amodeo II*, 71 F.3d at 1048.

[13] *Amodeo I*, 44 F.3d at 145-46 (characterizing the right as a "presumption favoring access to judicial records").

[14] *Amodeo II*, 71 F.3d at 1049.

[15] *Lugosch v. Pyramid Co. of Onondaga*, 435 F.3d 110, 120 (2nd Cir. 2006) (providing as examples of countervailing factors the "danger of impairing law enforcement" and "privacy interests of those resisting disclosure.") (internal quotation marks omitted).

[16] *Globe Newspaper Co. v. Superior Court for Norfolk Cty.*, 457 U.S. 596, 604 (1982) (internal citations and quotation marks omitted); *see also Richmond Newspapers*, 448 U.S. at 576 ("Free speech carries with it some freedom to listen.").

[17] *Globe Newspaper*, 457 U.S. at 604.

[18] *Richmond Newspapers*, 448 U.S. at 557 ("without the freedom to attend trials, . . . important aspects of freedom of speech and of the press could be eviscerated").

[19] *Globe Newspaper*, 457 U.S. at 605.

[20] Press-Enterprise Co. v. Superior Ct., 464 U.S. 501, 513 (1984) ("Press-Enterprise I").

[21] Press-Enterprise Co. v. Superior Ct., 478 U.S. 1, 11 (1986) ("Press-Enterprise II").

[22] *In re New York Times (Biaggi)*, 828 F.2d 110 (2d Cir. 1987).

To determine where the First Amendment right applies, courts analyze two factors: (1) whether the place and process have historically been open to the public, and (2) whether "public access plays a significant positive role in the functioning of the particular process in question."[26] When the First Amendment right of access attaches to a record, the record may be sealed only where closure is "necessitated by a compelling governmental interest, and is narrowly tailored to serve that interest."[27] This burden on the party seeking to prevent disclosure is higher than the burden created by the common law right of access.[28]

Courts are responsible for determining when the First Amendment access right is overcome.[29] To deny access the court must make factual findings on the record establishing that a probability of harm to some transcendent right justifies the limitation of the First Amendment right.[30] Those findings must be "specific enough that a reviewing court can determine whether the closure order was properly entered."[31] The fact that a sealing order has been entered must be docketed.[32] Lastly, the docket sheets themselves may not be sealed,[33] and a district court may not maintain a "dual-docketing system" wherein pretrial motions are "completely hid[den] from public view" in a non-public docket.[34]

---

[23] *In re Application of Nat'l Broad. Co.*, 635 F.2d 945, 952 (2d Cir. 1980).

[24] *In re Application of The Herald Co.*, 734 F.2d 93, 99 (2d Cir. 1984).

[25] *United States v. Haller*, 837 F.2d 84, 86 (2d Cir. 1988).

[26] Press-Enterprise II, 478 U.S. at 8-9.

[27] *Globe Newspaper*, 453 U.S. at 606-07.

[28] *Lugosch*, 435 F.3d at 126.

[29] *See Globe Newspaper*, 457 U.S. at 607-08 (rejecting a "mandatory closure rule" and affirming that trial courts must make sealing decisions on a "case-by-case basis").

[30] *In re Application of Herald Co.,* 734 F.2d at 100 ("The trial judge must articulate the basis for any closure order, supplying sufficient basis for appellate review.").

[31] *Press-Enterprise I*, 464 U.S. at 510.

[32] *Haller*, 837 F.2d at 87. *But see id*. ("The docketing of these matters may be delayed, however, in 'extraordinary situations' when an individual might be at risk.").

[33] *Hartford Courant Co. v. Pellegrino*, 380 F.3d 83, 86 (2d Cir. 2004).

[34] *United States v. Valenti*, 987 F.2d 708, 715 (11th Cir. 1993); *see also CBS, Inc. v. U.S. Dist. Court for Cent. Dist. Of California*, 765 F.2d 823, 826 (9th Cir. 1985) (observing that a "two-tier system, open and closed" erodes '[c]onfidence in the accuracy of [the court's] records.').

## II. Search Warrants and Electronic Surveillance Orders Are Judicial Records Subject to the Rights of Access

We will now describe the various types of warrants and orders that underlie our current concerns with the lack of access, and explain the basis for the public's qualified right to inspect these specific types judicial records.

*Rules governing warrants and surveillance orders.*

Physical Search Warrants. The warrant requirement for physical searches derives from the Fourth Amendment, which protects the "right of the people to be secure in their persons, houses, papers, and effects."[35] The warrant must be supported by probable cause and it must "particularly describe[e] the place to be searched."[36] Docketing and sealing procedures of warrants are governed by Rule 41 of the Federal Rules of Criminal Procedure.[37] That rule contains no provision regarding sealing.[38] Rather, Rule 41 requires magistrate judges to deliver a copy of the search warrant return to the clerk.[39] Absent exigent circumstances, law enforcement officers must provide notice to the subject of the search.[40]

Wiretap Orders. In contrast to physical searches, electronic surveillance is primarily governed by statute. For orders authorizing real time interception of the content of an individual's communications—wiretaps—the Wiretap Act requires a showing *higher* than probable cause.[41] Applications for wiretaps must contain detailed information, including "a full and complete statement of the facts and circumstances," as well as a showing that other investigative measures have been exhausted.[42] Wiretap applications and orders "shall be sealed by the judge," and "shall be disclosed only upon a showing of good cause."[43] The subject(s) of the wiretap must be notified of the wiretap's existence within ninety days after monitoring has terminated,[44] and both judges and government attorneys must submit annual reports detailing the number, nature, and outcome of wiretap applications.[45]

---

[35] U.S. CONST. Amend. IV.

[36] *Id*.

[37] Fed. R. Civ. P. 41.

[38] However, under 18 U.S.C. § 3103a(b)(3), notice of a warrant or other order may be delayed for 30 days, which has essentially the same effect as sealing.

[39] Fed. R. Civ. P. 41.

[40] *See Wilson v. Arkansas*, 514 U.S. 927, 936 (1995) (holding that police officers' failure to announce entry might render a search or seizure unconstitutional).

[41] 18 U.S.C. § 2510 *et seq*.

[42] *Id.* at § 2518(1).

[43] *Id.* at § 2518(8)(b).

[44] *Id.* at § 2518(8)(d).

[45] *Id.* at § 2519.

Section 2703(a) Warrants. For contents of communications that have been stored for less than one hundred and eighty days, § 2703(a) of the Stored Communications Act requires law enforcement officers to obtain a warrant supported by probable cause.[46] Section 2703(a) directs courts and law enforcement to follow the same Rule 41 procedures applicable to physical searches.[47]

Pen Register / Trap and Trace Orders. Lower standards apply when law enforcement seeks metadata surrounding an individual's communications, as opposed to the contents themselves. For example, to install a device that monitors an individual's outgoing calls (a pen register) or incoming calls (a trap and trace device), law enforcement need only certify that information "likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."[48] Orders for pen register or trap and trace devices must specify which criminal offense is related to the information that might be acquired through the installation of a pen register or trap/trace device.[49] They are automatically sealed "until otherwise ordered by the court."[50] Unlike subjects of wiretap orders[51] and physical searches, targets of pen register and trap & trace orders need not be given notice that they had been subject to surveillance.

Section 2703(d) Orders. To collect stored data metadata held by third parties (*i.e.*, cell phone companies), or content of communications that have been stored for over one hundred and eighty days, law enforcement need only show a court "that there are reasonable grounds to believe" that such information is "relevant and material to an ongoing criminal investigation."[52] These § 2703(d) orders have no other requirements, except that notice must be given if the order is used to compel disclosure of the contents of an individual's communications (as opposed to metadata).[53] The Pen/Trap Statute contains no provisions regarding sealing.[54]

When courts issue search warrants or orders for electronic surveillance, they are unquestionably performing Article III functions. So, while the origins and requirements of warrants and different types of orders differ, all are undeniably "judicial records."[55] Moreover, the affidavits that the government submits in support of search warrants and surveillance orders

---

[46] *Id.* at § 2703(a).

[47] *Id*.

[48] *Id.* at § 3123(a).

[49] *Id.* at § 3123(b)(1)(D).

[50] *Id.* at § 3123(d)(2).

[51] *Id.* at § 2518(8)(d) (2006) (requiring that targets of wiretap surveillance be notified "within a reasonable time but not later than ninety days" after the surveillance ends).

[52] *Id.* at § 2703(d).

[53] *Id.* at § 2703(b)(1)(B).

[54] Smith, *supra* note 5, at 325.

[55] *Amodeo I*, 44 F.3d at 146.

are documents "used in the performance of Article III functions,"[56] so they too qualify as "judicial records." With the exception of wiretap orders, all of these records are subject to the access rights provided by the common law and First Amendment.

*Application of the common law right.*

The Second Circuit has squarely held that the common law right of access attaches to search warrant materials.[57] In *Application of Newsday*, a newspaper sought access to the government's application for a warrant to search the home of a certain Mr. Gardner.[58] The order was executed after it was signed by a judge in the Eastern District of New York, but Mr. Gardner was never charged for a crime in the E.D.N.Y.[59] The government initially objected to unsealing the search warrant application, but it consented to unsealing after Mr. Gardner pled guilty to criminal informations filed in the Eastern District of Virginia.[60] Mr. Gardner, however, continued to object to unsealing, arguing that his privacy rights overrode any public right of access.[61]

The Second Circuit disagreed and held that the public had a common law right of access to search warrant materials.[62] The Court of Appeals found that the district court had appropriately balanced that right with Mr. Gardner's and others' privacy interests by redacting sensitive information from the search warrant materials.[63] Finding that the common law right of access attached to the records and was not overcome, the *Application of Newsday* court did not decide whether the First Amendment right of access also applies.[64]

The holding of *Application of Newsday* is not limited to warrants for physical searches. Because the issuance of §2703(a) warrants and orders for electronic surveillance are similarly "Article III functions,"[65] the common law right of access attaches to the warrants, orders, and

---

[56] *Id*.

[57] In re Application of Newsday, 895 F.2d at 74; accord United States v. Bus. of the Custer Battlefield Museum & Store, 658 F.3d 1188, 1194 (9th Cir. 2011); In re Eye Care Physicians of Am., 100 F.3d 514, 517 (7th Cir. 1996); In re Search of 1638 E. 2d Street, 993 F.2d 773, 775 (10th Cir. 1993).

[58] In re Application of Newsday, 895 F.2d at 75.

[59] *Id*.

[60] *Id*. The government admitted that the "need for secrecy is over" after the guilty plea was reached.

[61] *Id*. at 76.

[62] *Id*.

[63] *Id*. at 79-80.

[64] *Id.* at 75.

[65] *See Amodeo* II, 71 F.3d at 1048.

applications for electronic surveillance as well.[66] While the Second Circuit found that language within the Wiretap Act superseded the common law with respect to wiretap orders,[67] no such language exists in the statutes authorizing the other types of electronic surveillance outlined above.[68] Therefore, the common law right of access attaches to § 2703(a) warrants, Pen/Trap orders, and § 2703(d) orders.

*Application of the First Amendment right.*

The Second Circuit has yet to squarely address the application of the First Amendment access right to search warrants, but other circuit and district courts have.[69] Only one circuit court has examined whether the right attaches to 2703(d) orders, and that was only in the context of an ongoing grand jury investigation.[70] While the Second Circuit has held that wiretap orders are not subject to either right of access, [71] the court's reasoning in that case does not extend to the types of surveillance orders at issue. The governing "history and logic" test confirms that the constitutional access right does extend to such surveillance orders.

---

[66] *See In re Application of the U.S. for an Order Pursuant to 18 U.S.C. Section 2703(D)*, 707 F.3d 283, 291 (4th Cir. 2013) (holding that § 2703(d) orders are "judicial records" subject to the common law right of access).

[67] *In re New York Times Co. to Unseal Wiretap & Search Warrant Materials*, 577 F.3d 401 (2d Cir. 2009) (finding that a provision allowing unsealing "only upon a showing of good cause" displaced the common law presumption of access)

[68] The Wiretap Act is unique in that it provides that orders and applications "shall be disclosed only upon a showing of good cause." 18 U.S.C. § 2518(8)(b). By contrast, § 2703(d) does not address sealing or unsealing at all, and the Pen/Trap stature provides only that Pen/Trap orders shall be sealed "until otherwise ordered by the court." 18 U.S.C. § 3123(d)(2). Initial sealing, of course, is consistent with practices surrounding physical search warrants, and there is no language within the Pen/Trap statute to suggest that the common law right of access would be an insufficient reason for a court to order unsealing.

[69] *See In re Search Warrant for secretarial Area Outside the Office of Thomas Gunn*, 855 F.2d 569 (8th Cir. 1988) (qualified constitutional right of access to search warrant applications once the warrant had been executed, even if the investigation had not been completed); *In re Application of N.Y. Times Co.*, 585 F. Supp. 2d 83 (qualified right of access to warrant materials after the investigation has concluded). *Contra, In re Search of Fair Finance*, 692 F.3d 424 (6th Cir. 2012) (no right of access to warrant materials even after conclusion of investigation); *Baltimore Sun Co. v. Goetz*, 886 F.2d 60 (4th Cir. 1989) (no right of access during investigation, declining to decide whether right attaches after investigation concludes); *Times Mirror Co. v. United States*, 873 F.2d 1210, 1221 (9th Cir. 1989) (same).

[70] *In re U.S. for an Order Pursuant to 18 U.S.C. Section 2703(D)*, 707 F.3d 283 (4th Cir. 2013) (concluding that the right does not attach to § 2703(d) orders while an investigation is ongoing).

[71] See In re New York Times Co. to Unseal Wiretap & Search Warrant Materials, 855 F.2d at 573.

*1. History.*

To satisfy the "experience" prong, an unbroken tradition of access is not necessary: "near uniform practice suffices."[72] In federal courts today, "search warrant applications and receipts are routinely filed with the clerk of court without seal."[73] Indeed, Rule 41(i) requires magistrate judges to deliver a copy of the search warrant return to the clerk, presumably for the clerk to file for public inspection.[74] Moreover, allowing public access to search warrants is consistent with colonial legislators' repudiation of secret searches,[75] as well as the Fourth Amendment's preference for open searches.[76] Thus, while the process of issuing search warrants is not conducted in an open fashion, the results of that process—the search warrants themselves, including the government's affidavits in support—have been open to inspection by the public.[77]

Of course, there is no long-term history of access to §2703(a) warrants, Pen/Trap orders, or §2703(d) orders, because those records did not exist before the Stored Communication Act was passed in 1986. In such circumstances involving court records created by new statutory obligations, the Second Circuit has found that satisfying the history prong of the *Press Enterprise II* is not essential. In *U.S. v. Suarez*, 880 F.2d 626, 631 (2d Cir. 1989) the court expressly held that the First Amendment right attaches to records filed to comply with the Criminal Justice Act, notwithstanding the lack of any "tradition of accessibility" because the type of records at issue did not exist before 1964. [78]

---

[72] *Press-Enterprise II*, 478 U.S. at 10.

[73] In re Search Warrant for Secretarial Area Outside Office of Gunn, 855 F.2d at 573.

[74] *Baltimore Sun Co. v. Goetz*, 886 F.2d 60, 64 (4th Cir. 1989) ("Frequently—probably most frequently—the warrant papers including supporting affidavits are open for inspection by the press and public in the clerk's office after the warrant has been executed"); *In re search Warrant for Secretarial Area Outside Office of Gunn*, 855 F.2d at 573 ("[S]earch warrant applications and receipts are routinely filed with the clerk of court without seal."); *In re Application of N.Y. Times Co. for Access to Certain Sealed Court Records*, 585 F. Supp. 2d at 88 n.8 ("The Court has been advised by the clerk's office in the United Stated District Court fo the District of Columbia that the routine practice is to make warrant materials publicly available after a search has been executed and a return is available.").

[75] *See* CUDDIHY, THE FOURTH AMENDMENT 660-61 (describing colonial legislators' abhorrence for measures that would facilitate secret searches, such as no-knock entry and nocturnal surveillance).

[76] *See Wilson v. Arkansas*, 514 U.S. 927 (1995) (holding that law enforcement's adherence to the knock-and-announce rule factors into courts' inquiry into the "reasonableness" of searches).

[77] See In re Search Warrant for Secretarial Area Outside Office of Gunn, 855 F.2d at 573.

[78] *See also U.S. v. Simone*, 14 F.3d 833, 838 (3d Cir. 1994) (finding that the "experience" prong of the "logic and experience" test provided little guidance and relying "primarily" on the logic prong).

Similarly, the absence of a long history of access was not dispositive in *NYCLU v. N.Y. City Transit Authority*, which found the constitutional right of access to extend to certain administrative proceedings.[79] Judge Calabresi recognized that "widespread administrative adjudication is a relatively new phenomenon," and, if the history test were applied formulaically, administrative records would fail this part of the *Press-Enterprise II* test.[80] But "changes in the organization of government do not exempt new institutions from the purview of old rules. Rather, they lead [courts] to ask how the new institutions fit into existing legal structures."[81] Otherwise, legislatures could "avoid constitutional strictures by moving an old governmental function to a new institutional location."[82] Therefore, the Second Circuit found that the lack of history to administrative adjudications is not dispositive; instead, the court analogized those adjudications to court proceedings and held that the same right of access applies in both instances.[83]

Similar reasoning dictates a similar result here: warrants under § 2703(a) and surveillance orders under §2703(d) and the pen register and trap and trace acts play the same role as physical search warrants. The relevant historical inquiry, therefore, is not the history of access to these statutorily-created records themselves, but the history of public access to search warrants generally. And, as described above, the history of search warrants is one of public disclosure.

*2. Logic.*

The logic prong of the *Press-Enterprise II* test heavily favors the right of access attaching to search warrants and surveillance orders. A "search warrant is certainly an integral part of a criminal prosecution,"[84] and "public access plays a significant positive role in the functioning of the particular process in question."[85] In this case, the particular process is constitutionally-mandated judicial oversight of law enforcement investigatory practices. Some aspects of that process rightfully require secrecy, but significant benefits accrue from disclosing warrants along with their supporting evidence. Public access to these records "operate[s] as a curb on prosecutorial or judicial misconduct."[86] If infirm warrants are allowed to remain sealed forever, prosecutors are more likely to submit insufficient warrant applications, and magistrate judges are more likely to serve as rubber stampers if they are less likely to face consequences for issuing an invalid warrant. Public access to these records is likely to play "a significant positive role" in the warrant process.

---

[79] 684 F.3d 286, 290 (2d Cir. 2012).

[80] *Id*.

[81] *Id*.

[82] *Id*.

[83] *Id*.

[84] In re Search Warrant for Secretarial Area Outside Office of Gunn, 855 F.2d at 573.

[85] Press-Enterprise II, 478 U.S. at 8-9.

[86] In re Search Warrant for Secretarial Area Outside Office of Gunn, 855 F.2d at 573.

Moreover, public access to search warrants is necessary "to ensure that th[e] constitutionally protected discussion of governmental affairs is an informed one."[87] If search warrants remain perpetually sealed at the government's discretion, the public will only be able to monitor a subset of the orders issued—those that bear fruit and are used in a criminal prosecution. Government watchdogs would have no way of uncovering discriminatory searches that do not eventuate in criminal prosecutions. Searches that ultimately fail to produce indictments or admissible evidence are potentially more likely to contain constitutional infirmities. Public access to search warrants and their supporting affidavits will increase public confidence that the judiciary is striking the proper balance between privacy rights and law enforcement exigencies.

These benefits of disclosure are magnified with respect to electronic surveillance orders. With the exception of wiretaps, such orders require a *lesser* showing than probable cause.[88] Therefore, the potential for misconduct is increased because law enforcement can more easily target individuals without cause. Also, the lesser showing means that citizens are likely to have less confidence that "judges are not merely serving as a rubber stamp for the police."[89] Moreover, unlike with warrants and wiretaps, searches pursuant to the Pen/Trap Acts and non-content searches pursuant to § 2703(d) do not require the subject of the searches to be notified. Mandating access to these surveillance orders will bring them into the open, consistent with both legislators' and courts' distrust of secret searches.[90] Lastly, because so many § 2703(d) and Pen/Trap orders are sealed, the public does not know whether these statutes are being used to authorize the use of new technologies such as "cell site simulators," also known as StingRays, which collect information from cellphones. The public cannot sustain an informed debate about the appropriate use of these new technologies if citizens have no way of knowing how often and under what authority they are used.[91]

Of course, there are undeniably competing interests that militate against disclosure. The danger of compromising a criminal investigation is significant, at least while the investigation is ongoing. Post-investigation, however, that danger usually dissipates.[92] What remains is the privacy interest of the individual who has been subjected to a search. But that privacy interest cannot categorically trump the public's First Amendment access right; rather, courts should balance privacy rights with the need for transparency on a case-by-case basis by redacting sensitive information.[93]

---

[87] *Globe Newspaper Co*, 457 U.S. at 604-05.

[88] *See* pages 5-6, *supra*.

[89] *In re Application of N.Y. Times Co*, 585 F. Supp. at 90 (citing *U.S. v. Leon*, 468 U.S. 897, 917 n.18 (1984)).

[90] *See* note 75, *supra*.

[91] *See Globe Newspaper Co*, 457 U.S. at 604-05.

[92] *See In re Application of Newsday*, 895 F.2d at 75 (government recognizing that "the need for secrecy" was over after the investigation concluded).

[93] Though Congress may have balanced the access right with privacy rights by creating a "statutory presumption against disclosure" in the Wiretap Act, *In re New York Times Co. to*

*At the Very Least, the First Amendment Requires Docketing*

A failure to docket electronic search warrant materials raises additional concerns and likely violates the docketing requirement of *Hartford Courant Co. v. Pellegrino*.[94] If search warrant materials are not even docketed, the public cannot determine even *how many* searches have been authorized. Nor can it estimate what percentage of electronic searches lead to evidence of criminal misdoing. Because neither the Pen/Trap Act nor § 2703(d) require notice to targets of electronic surveillance, it is all the more important that such orders be docketed so that the public is aware of the extent of government surveillance, particularly when such surveillance is of innocent people and is unrelated to criminal charges. Thus, while the government may rightly seal surveillance orders for some period of time, the fact that such orders have been sealed must be docketed.

The benefits of transparency surrounding searches is exemplified by New York City's experience with widespread "stop and frisk" searches. At its height in 2011, New York police conducted 685,724 stop-and-frisk searches.[95] The vast majority of those searches targeted black and Latino individuals, and 88% of searches revealed no criminal evidence.[96] As data surrounding such stops became publicly available, citizens expressed their dissatisfaction[97] and voted in a mayor who promised to reform the police practices.[98] By 2015, the number of searches was down to 22,939—a 97% decrease from 2011.[99] Transparency regarding the number and targets of searches undoubtedly played a large role in reform.[100]

* * *

---

*Unseal Wiretap & Search Warrant Materials*, 577 F.3d at 410, no such statutory presumption exists in § 2703(d) or the Pen/Trap statute. So, while it may be appropriate for courts to defer to Congress's judgments in the case of wiretaps, courts cannot must conduct the balancing themselves in the cases of § 2703(d) and Pen/Trap orders.

[94] 380 F.3d at 86.

[95] New york Civil Liberties Union, Stop-and-Frisk Data, https://www.nyclu.org/en/stop-and-frisk-data.

[96] Id.

[97] Chris Francescani, Silent March to Protest NYPD's 'Stop-and-Frisk' Policy, REUTERS.COM, (June 17, 2012), http://www.reuters.com/article/us-usa-newyork-march-idUSBRE85G0A920120617.

[98] A. Paybarah, B. Cheney & C. Hamilton, De Blasio on Stop-and-Frisk: "We Changed It Intensely," POLITICO (Dec. 8, 2016), http://www.politico.com/states/new-york/city-hall/story/2016/12/de-blasio-on-stop-and-frisk-we-changed-it-intensely-107886.

[99] *See* New York Civil Liberties Union, *supra* note 95.

[100] In the stop-and-frisk case, the NYPD collected and released data on its own accord. In that case, the judiciary had little role to play because stop-and-frisk searches do not require warrants. *See Terry v. Ohio*, 392 U.S. 1 (1968). Here, by contrast, the search warrant and surveillance order requirements invite the judiciary to play a more active role in fostering transparency.

The purpose of physical search warrants and electronic surveillance orders are the same: they allow a third party to evaluate whether the government is justified in invading privacy rights. Issuing physical search warrants and electronic surveillance orders are clearly "Article III functions,"[101] so both the common law and the First Amendment grant the public a qualified right of access to search these materials. The benefits of transparency that the Second Circuit described in *Amodeo II* apply in equal force here: transparency will allow public monitoring of decisions to issue search warrant orders, which in turn will improve judicial decision-making and increase public confidence in the system of justice.[102] In the need for transparency, there is no meaningful distinction between physical search warrants—which the Second Circuit has held to be subject to the common law access rights[103]—and electronic surveillance orders. Indeed, because electronic surveillance warrants may be obtained with a *lower* showing of cause than that required for physical search warrants, access to such materials is even *more* important.[104]

## III. Sealing Practices in Connecticut District Courts.

Connecticut's Local Rule of Criminal Procedure 57(b) ("L.R. 57(b)") contains a relatively detailed regime for sealing proceedings and documents, which sets forth sealing standards and docketing and handling directions for a variety of court records. Discussions with attorneys from the Criminal Division of the United States Attorney's Office for the District of Connecticut and the Clerk's Office of the New Haven Courthouse revealed more about how this rule is put into practice. Specifically, it is apparent that the sealing of criminal indictments and cases is routinely extended, that the USAO makes unsealing decisions on an *ad hoc* basis, and that there is no systematic means for the public to find unsealed applications for search warrants on ECF.

However, this District's use of ECF furthers transparency goals and access rights, as compared to districts that continue to use paper filing systems. Much of our research would have been immensely time-consuming, or completely impossible, without the ability to search through electronic dockets. On the government's side, the potential to generate automated reminders regarding a case's status or upcoming deadlines increases the ease of implementing unsealing procedures along the lines proposed in Section IV below.

---

[101] *See Amodeo* II, 71 F.3d at 1048.

[102] *Amodeo II*, 71 F.3d at 1048.; *see also In re Application of N.Y. Times Co.*, 585 F. Supp. 2d at 90 ("Public access to warrant materials serves as a check on the judciciary because the public can ensure that judges are not merely serving as a rubber stamp for the police."); *In re Search Area Outside Office of Gunn*, 855 F.2d at 573 (warrant materials are "important to the public's understanding of the function and operation of the judicial process and the criminal justice system and may operate as a curb on prosecutorial or judicial misconduct").

[103] In re Application of Newsday, 895 F.2d at 74.

[104] See In re Application of N.Y. Times Co, 585 F. Supp. at 90.

*Current Practice Pursuant to Local Rule 57(b)*

Wiretap applications, supporting documents, orders addressing wiretap applications, and "fruits" of wiretaps are maintained by the United States Attorney's Office or its designee.[105] For orders authorizing pen registers and trap and trace, and any supporting documents, a "miscellaneous sealed case" is opened.[106] The docket will note "Pen Register [or Trap and Trace] filed." *Id*. Search warrants, applications, and supporting documents are maintained by the authorizing judicial officer until the warrant is executed and returned.[107] Search warrant returns are not sealed except for "sufficient cause." *Id*. The United States Attorney's Office may, however, request that the judicial officer hold pen register, trap and trace, or search warrant documents "for a reasonable period of time (*i.e*., until the related criminal case has been charged and publicly disclosed)" before delivering them to the clerk for filing.[108]

Discussions with Assistant United States Attorneys in the Criminal Division of the Connecticut office revealed that their office has not implemented any unsealing procedures of its own. With regards to search warrants in particular, but also other surveillance authorizations, the Attorneys stated that unsealing is heavily fact- and case-specific, and that they were unable to say in general or give examples of circumstances in which they would move to unseal. They also noted that there is no rule or practice on returning authorized search warrants that were not ultimately executed. The decision whether to seek unsealing of these documents in a particular case appears to be delegated to the Attorney handling that case.

We also learned that, consistent with L.R. 57(b)(7)(d), the Clerk's office does not receive search warrant documents until the warrant has been executed and returned. If those records are subsequently unsealed, they are filed and docketed on ECF. The office also stated that pen register documents are never unsealed, and they do not appear on ECF at all.

One can find unsealed search warrant applications by running a search for all criminal cases without filters. The Clerk's office stated that most, if not all, applications go to magistrate judges, so searching only for magistrate judge cases will also return a number of unsealed applications. Most of the results of these reports, however, are cases captioned "Sealed v. Sealed." While the Attorneys with whom we spoke were unsure of the nature of these entries, one of them speculated that they might be sealed search warrants and other magistrate judge rulings. The Clerk's office indicated the same.

It is also possible to run a query for unsealed applications, but because they are not consistently captioned, it is not possible to perform a comprehensive search for these documents. The plaintiff will always be listed as the United States, but we observed a wide range of defendants. Often, it is simply "Search Warrant," but it may also be a mail parcel—with several subtly different naming conventions such as "U.S. Priority Mail Parcel" or "Priority Mail Parcel"

---

[105] L.R. 57(b)(7)(b).

[106] L.R. 57(b)(7)(c).

[107] L.R. 57(b)(7)(d).

[108] L.R. 57(b)(7)(c)-(d).

and only sometimes including the tracking number or addressee—a mail tracking number standing alone, an address, or a computer model. The Clerk's office stated that, in recent years, it has standard procedure to caption these cases "U.S.A. v. Search Warrant," but we observed other naming conventions in cases from 2016. For example, mail parcels may be named differently and may not include a tracking number or the addressee, while addresses are not always given in a common format. This makes it impossible to run a query for a specific search warrant without knowing in advance the exact naming convention used, impossible to run a query for a specific warrant that has been captioned in the standard manner, and impossible to run a search for all unsealed warrants. Because warrant applications come before magistrate judges, it is possible to alleviate the last of these consequences by running a report only for those cases, but this is still over-inclusive.

While L.R. 57(b) establishes relatively comprehensive sealing procedures, it is largely silent on unsealing. Except for sealed indictments, which must be unsealed upon the first defendant's initial appearance,[109] L.R. 57(b) imposes no unsealing procedures or requirements of any kind. Unsealing is left to motion by the parties or an intervenor, sua sponte order of the court, or appeal from either of the former.[110] In addition, while L.R. 57(b) requires sealing of documents to be justified by particularized findings of a compelling interest and narrow tailoring, it offers no guidance as to when unsealing is justified.[111]

A rough count indicated that approximately 1/6 of all criminal cases in which documents were filed between January 1, 2000 and February 22, 2017 are listed as "Sealed v. Sealed." For cases before magistrate judges from the same period, this rises to approximately 1/3. Roughly two thousand cases from 2016 are docketed in this way, about 1,100 from 2015. The number continues to decline back in time to cases from 2003 and earlier, of which roughly 60 per year remain sealed.

## IV. Recommendations.

L.R. 57(b) currently permits routine, indefinite sealing of documents, as well as the very findings the rule requires to justify sealing in the first place—and this appears to be precisely what occurs in the District of Connecticut. This is particularly evident with regard to search warrant and surveillance materials.

This state of affairs infringes upon the public's right of access to judicial documents.[112] While a finite sealing period is no doubt justified in instances where personal and law enforcement information are at stake, such information must or may be redacted when documents become available to the public under the District's Privacy Policy.[113] The current

[109] L.R. 57(b)(2).

[110] L.R. 57(b)(6), (b)(9).

[111] L.R. 57(b)(3).

[112] See supra Part I.

[113] *See* Privacy Policy, United States District Court, District of Connecticut, Feb. 28, 2012, *http://www.ctd.uscourts.gov/sites/default/files/PRIVACY%20POLICY%202-28-12.pdf*.

practice of maintaining so many documents under seal indefinitely undermines the public's ability to monitor and its confidence in the surveillance apparatus, and criminal justice system as a whole.[114] Inconsistent docketing practices and the difficulty of finding search warrant applications on PACER—both systematically and specifically—impairs practical exercise of the access right. And the wholesale sealing of dockets clearly violates the First Amendment.[115]

**Recommendation 1: Incorporate a Sunshine Provision for all Search Warrants and Surveillance Orders**

L.R. 57(b)(9) should be amended to include a sunset for sealing orders for search warrant and surveillance materials. Examples from several other United States District Courts make clear that it would be both simple and realistic to amend L.R. 57(b) to address over- and overlong sealing. The local rules of other courts provide several different models for such a provision. Additionally, the Clerk's Office should adopt specific, uniform docketing and naming conventions for unsealed applications and orders.

The rules of at least five United States District Courts and one territorial court currently provide that applications for search warrants will be unsealed by default upon the warrant's return or after a finite period of time. We recommend that this District adopt such an approach by amending L.R. 57(b) to include a definite "sunshine" date for search warrants and electronic surveillance orders.

- The Western District of New York's Local Criminal Rule 41 provides that applications and warrants are to be filed under seal. However, "the entire matter, including the application and search warrant," is to be unsealed after the earlier of twenty-eight days since the warrant's issuance and the warrant's return along with an inventory. The government may request sealing for a "specific period of time . . . , until further order of the Court, or as the Court otherwise directs." While this rule still permits the government to request and the court to grant indefinite sealing, "the entire matter" is unsealed by default.

- The Western District of North Carolina's Local Criminal Rule 55.1(G) states that "application[s] for arrest, search, and seizure warrant[s] shall be sealed until all the warrants have been executed and returned to the Court." The government, defendant, and interested parties may move to unseal prior to execution or return. The government may move to continue the seal after execution. As in the W.D.N.Y., this default unsealing rule still allows for indefinite sealing.

- The Northern District of Illinois's Local Criminal Rule 41(d) supplies specific sealing provisions for search and seizure warrants. The government must move to seal the warrant and specify a date, at most ninety days later, at which the sealing order and all other filings will expire "absent a further court order." The government may move to extend the sealing order under Rule 41(e). While this

[114] *See Amodeo II*, 71 F.3d at 1048.

[115] Hartford Courant Co., 380 F.3d at 96.

rule, too, makes indefinite sealing possible, the government must affirmatively move to bring it about.

- The District of Maine's Local Rule 157.6(a)(1) specifies that search and tracking warrant applications, affidavits, and warrants are to be automatically sealed upon filing, but only "until the warrant is executed and returned to the Court." There is no reference to continued sealing.

- The Northern District of Oklahoma's Local Criminal Rule 41.1 provides that supporting affidavits for search, seizure, and tracking warrants, as well as the warrant themselves, shall be filed under seal. But upon the warrant's return, the application, affidavits, inventory, and warrant are to be unsealed unless the government moves, and the court orders, sealing. The duration of the sealing is not discussed.

- Finally, the District of Guam's Criminal Local Rule 41(b) provides that search and seizure warrants are to be unsealed, along with "any other document contained in the file" upon the warrant's return, unless the government moves for sealing. Such motions are to be granted only for "good cause shown" and the government "can demonstrate that sealing is necessary and essential to preserve the integrity of an ongoing investigation or case." The duration of the sealing is not discussed.

**Recommendation 2: Unseal Search Warrants Upon Return**

Search warrants and other orders that are returned to the presiding judge or magistrate judge after execution should, by default, be unsealed upon return. The local rules described above supply several templates, but all provide for default unsealing upon a warrant's return.

Surveillance orders that are not returned after execution, such as pen registers and trap and trace orders, should be unsealed by default after ninety days. The government should be able to move to extend sealing for an additional ninety days. This would treat sealing of these orders commensurately with the delayed notice provisions contained in 18 U.S.C. § 2705.

**Recommendation 3: Implement Time Limits for Extensions of Sealing Orders**

The government should be able to move to continue sealing where the warrant or order is related to an ongoing investigation or where sufficient cause would otherwise justify continued sealing. This additional sealing period should also be definite, as indefinite sealing generally cannot be justified where a First Amendment right of access exists.[116] This rule would allow for further sealing where necessary, but only after the government satisfies a meaningful standard.

**Recommendation 4: Adopt a Standard Docketing Convention**

The Court's docketing and filing system should accomplish the following in order to comply with and facilitate the public's right of access: public docketing of search warrant and surveillance materials; docketing the grant of sealing orders; a clear and consistent naming convention; public notice of unsealing; and automatic reminders to the United States Attorney's Office. We offer three possible procedures that would, together, accomplish these goals.

Listing the defendant in a search warrant case as the object or location searched with the greatest possible specificity would greatly reduce the burden of searching for a specific search warrant by obviating the need to inspect the filings in each particular case. Specifically naming the object of the search would best allow those seeking a specific warrant to exercise their First Amendment right of access. Where a warrant or surveillance order has not resulted in an indictment, it would be proper to redact or omit names and other identifying information.

The ECF system could also allow the Clerk's office to tag these cases as warrants and surveillance orders so that one may run a filtered report for them. This would best allow those seeking to monitor the administration of criminal justice in this District to comprehensively evaluate the issuance and execution of these warrants and orders. Tagging matters in this way would also aid in the administration of the unsealing procedures proposed above by automating public notice of unsealing, as well as reminders and alerts to the United States Attorney's Office in cases with approaching unsealing deadlines.

Moreover, the Court could maintain a docket that lists all sealing orders that relate to search warrants and surveillance orders. Such a system, which is already in place in the Northern District of New York,[117] would allow citizens to monitor the scope of surveillance activity, and it would allow interested individuals to move to unseal individual cases.

*Proposed Amendments to Local Rule 57(b)*

The following proposed changes to L.R. 57(b) incorporate our recommendations based on our analysis of current rules and practices in the District of Connecticut and in other federal district courts, as well as our analysis of the First Amendment right of access to judicial documents.

L.R. 57(b)(7)(c) Pen registers/trap and trace.

> Orders authorizing pen registers or trap and trace of telephone calls, along with related applications and supporting documents, shall be delivered to one of the criminal docket clerks in the Office of the Clerk upon approval by a judicial officer. If no criminal docket clerk is available, the papers shall be delivered to an office supervisor. The papers submitted will be

[117] *See, e.g., In re: Sealing Order(s) for Public Filing*, 5:17-sp-02017 (N.D.N.Y. 2017) (listing all public sealing orders issued thus far in 2017); *USA v. Sealing Order(s) for Public Filing*, 5:16-sp-02016 (N.D.N.Y. 2016) (listing all such orders in 2016).

filed stamped and a miscellaneous sealed case will be opened, with the docket entry reflecting "Pen Register filed" or "Trap and Trace filed." ~~At the request of the United States Attorney's Office, pen register/trap and trace orders, along with related applications and supporting documents, may be held by the judicial officer for a reasonable period of time (i.e., until the related criminal case has been charged and publicly disclosed) prior to presentation to the Clerk's Office for filing.~~ After ninety days have passed, the matter shall be unsealed, except that the United States Attorney's Office may submit a motion requesting that the matter remain sealed for an additional ninety days.

L.R. 57(b)(7)(d) Search Warrants.

Copies of search warrants, along with the search warrant application and supporting affidavits or other papers, shall be maintained by the judicial officer authorizing the warrant until the warrant has been executed and returned, at which time the warrant papers shall be filed with the Clerk. ~~At the request of the United States Attorney's Office, search warrants, along with search warrant applications and supporting affidavits or other documents may be held by the judicial officer for a reasonable period of time (i.e., until the related criminal case has been charged and publicly disclosed) prior to presentation to the Clerk's Office for filing.~~ The matter, including supporting warrants and affidavits, shall be unsealed upon the warrant's return, unless the United States Attorney's Office submits a motion requesting that the warrant remain sealed because it is related to an ongoing investigation or for sufficient cause, in which case the matter will remain sealed for ninety additional days. In extraordinary circumstances, the United States Attorney's office may request further, definite sealing. Unless otherwise directed by the Court for sufficient cause, search warrant returns shall be docketed as unsealed filings.

L.R. 57(b)(9)

Except as provided above, ~~A~~any case or document ordered sealed by the Court shall remain sealed pending further order of this Court, or any Court sitting in review. Upon final determination of the action, as defined in Rule 83.6(c) of the Local Rules of Civil Procedure, counsel shall have ninety (90) days to file a motion pursuant to Rule 83.6(a) for the withdrawal and return of sealed documents. Any sealed document thereafter remaining shall be destroyed by the Clerk pursuant to Rule 83.6(e) prior to the delivery of other parts of the file to the Federal Records Center. The return or destruction of hard copies of sealed documents shall not serve to unseal electronic copies of documents sealed by Court order.

## Conclusion

Citizens have a right of access to judicial records under both the common law and the First Amendment, and that right extends to search warrants and electronic surveillance orders. This right serves critical democratic interests in the ability of citizens to monitor, and thus maintain confidence in, law enforcement activity and its attendant judicial proceedings. The widespread, indefinite sealing of search warrant and surveillance materials in the District of Connecticut curtails the exercise of that right and subverts that interest. To best protect the essential public right of access, the District should adopt rules that would unseal search warrant and surveillance materials after a default, definite period of time, except where the government has shown cause, and docket these orders in a uniform manner providing the greatest amount of information in the first instance.

A.U.
Y.M.