

**IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF TENNESSEE  
WESTERN DIVISION**

---

ACLU OF TENNESSEE, Inc.	)	
	)	
Intervening Plaintiff,	)	
v.	)	No. 2:17-cv-02120-jpm-DKV
	)	
THE CITY OF MEMPHIS,	)	
	)	
Defendant.	)	

---

**THE CITY’S MOTION FOR CONTINUANCE AND/OR A STAY OF FILING  
QUARTERLY SUBMISSION OF SEARCH TERMS IN LIGHT OF RECENT  
CYBERSECURITY ISSUES**

The Defendant, the City of Memphis ("the City"), files this Motion for Continuance and/or a Stay of Filing Quarterly Submission of Search Terms in Light of Recent Cybersecurity Issues with the Court’s CM/ECF system. In support, the City states as follows:

**I. Background on Sanction 5**

Pursuant to the Court’s October 27, 2018 Opinion and Order, ECF No. 151, the Court imposed certain sanctions on the City and ordered compliance by a date certain. (ECF No. 151.)

The Court required, in part, that:

5) The City shall maintain a list of all search terms entered into social media collators or otherwise used by MPD officers collecting information on social media while on duty. This list shall be filed under seal every three months until the Court orders otherwise. The first filing shall be submitted no later than January 14, 2019 and shall reflect all such social media searches conducted from November 1, 2018 through December 31, 2018.

(“Sanction 5”) (ECF No. 151, PageID 6275.)

Pursuant to Sanction 5, the City began collecting search terms from Memphis Police Department (“MPD”) officers in certain investigative units. The City submitted the search terms

reported from those units to the Court under seal every quarter beginning in January 2019 through July 2020.

In an August 19, 2020 Order, the Court ordered the City to disclose all work-related social media search terms used by all MPD officers, including the officers from the Multi-Agency Gang Unit (“MGU”), the Organized Crime Unit (“OCU”), and the Internet Crimes Against Children (“ICAC”) divisions, under seal, as part of its quarterly filings. (ECF No. 363, PageID 12306.) The Court also ordered the City to supplement its previous filings with the work-related search terms since January 2019 from the officers it had not previously reported. (*Id.*)

In the August 19, 2020 Order, the Court noted the City’s objection to the disclosure of certain search terms over security concerns, but ruled that filing the search terms under seal was sufficient to “protect[] sensitive law enforcement information from inadvertent public disclosure while providing a formal mechanism to protect the individual liberty and the integrity of agreed upon restrictions in the Kendrick Decree.” (ECF No. 363, PageID 12305.)

On October 19, 2020, pursuant to the Court’s August 19, 2020 Order, the City submitted its latest collection of search terms under seal. (*See* ECF No. 383.) The City’s next quarterly submission of search terms is due January 14, 2021. The City has collected those search terms from its officers and stands ready to produce them.

## **II. The recent security breach of the Court’s CM/ECF system.**

On January 6, 2021, the City learned that the Judicial Conference of the United States issued a Memorandum notifying the federal court system of a significant cybersecurity breach of the Court’s Case Management/Electronic Case Filing (CM/ECF) system. (“Judicial Conference Memorandum,” attached as **Exhibit A**.) The Judicial Conference Memorandum asks all federal courts to issue a standing or general order or to adopt some other equivalent procedure requiring

that highly sensitive documents (“HSDs”) will be accepted for filing only in paper form or via a secure electronic device. The Judicial Conference Memorandum notes that not every sealed document should be considered a HSD, and courts should use their discretion in determining which documents require HSD protection.

Additionally, the Judicial Conference Memorandum explains that any document pertaining to a HSD, i.e. filing, order, etc., should not be uploaded to the CM/ECF or PACER systems or to any system connected to a network or the internet. The Judicial Conference Memorandum further directs that litigants may request certain sealed documents be removed from CM/ECF expeditiously.

To date, the City is not aware of any standing order or equivalent procedure issued by this Court providing guidance on how to proceed with filing Highly Sensitive Documents — which the City believes its search term submissions to be — under seal going forward.

In view of the above, the City seeks a continuance and/or a stay of the filing of its January 14, 2021 submission of search terms under seal until it receives guidance from the Court by way of a standing Order or specific guidance related to the City’s sealed search terms submissions.

Respectfully Submitted,

BAKER, DONELSON, BEARMAN,  
CALDWELL & BERKOWITZ, P.C.

s/ Bruce McMullen

---

R. Mark Glover (#6807)  
Bruce McMullen (#18126)  
Mary Wu Tullis (#31339)  
Jennie Vee Silk (#35319)  
165 Madison Avenue, Suite 2000  
Memphis, Tennessee 38103  
Telephone (901) 526-2000  
E-mail: [bmcmullen@bakerdonelson.com](mailto:bmcmullen@bakerdonelson.com)

mglover@bakerdonelson.com  
mtullis@bakerdonelson.com  
jsilk@bakerdonelson.com

*Attorneys for Defendant, The City of  
Memphis*

**CERTIFICATE OF CONSULTATION**

Pursuant to Local Rule 7.2(a) (B), on January 13, 2021, counsel for the city, Jennie Silk, conferred with counsel for Intervening Plaintiff, Thomas Castelli, by email regarding the relief sought in this Motion. The ACLU-TN does not oppose the relief the City seeks with this Motion.

s/ Bruce McMullen  
\_\_\_\_\_  
Bruce McMullen

**CERTIFICATE OF SERVICE**

I hereby certify that on January 13, 2021, the foregoing document will be served by the Court's CM/ECF system to:

Thomas H. Castelli  
Stella Yarbrough  
ACLU Tennessee, Inc.  
P.O. Box 120160  
Nashville, TN 37212  
tcastelli@aclu-tn.org  
syarbrough@aclu-tn.org

Mandy Strickland Floyd  
Bone McAllester Norton PLLC  
511 Union Street, Suite 1600  
Nashville, Tennessee 37219  
mfloyd@bonelaw.com

*Attorneys for Intervening Plaintiff*

s/ Bruce McMullen  
\_\_\_\_\_

# EXHIBIT A



JUDICIAL CONFERENCE OF THE UNITED STATES

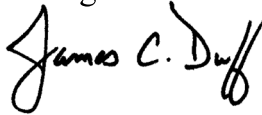
WASHINGTON, D.C. 20544

THE CHIEF JUSTICE  
OF THE UNITED STATES  
*Presiding*

JAMES C. DUFF  
*Secretary*

January 6, 2021

MEMORANDUM

To: All United States Judges  
From: James C. Duff   
RE: POLICY CHANGE FOR SEALED FILINGS IN CM/ECF  
(URGENT ACTION REQUIRED)

Recent news reports revealed significant cybersecurity breaches into the computer systems of federal agencies. These reports indicate that the breaches possibly were caused by nation state actors as part of a global espionage campaign with confirmed instances of compromise of highly sensitive information in those systems. The Administrative Office of the U.S. Courts (AO) is working with the Department of Homeland Security on a security audit of our most sensitive and critical computer application, the Case Management/Electronic Case Filing (CM/ECF) system. This action is endorsed by the Judicial Conference's Executive Committee and supported by the Conference's Information Technology and Court Administration and Case Management Committees. That audit indicates serious security vulnerabilities in CM/ECF that greatly risk compromising highly sensitive non-public documents stored on CM/ECF, particularly sealed filings. An apparent compromise of the confidentiality of the CM/ECF system due to these discovered vulnerabilities currently is under investigation.

The Federal Judiciary has long applied a strong presumption in favor of public access to documents. Court rules and orders should presume that every document filed in or by a court will be in the public domain, unless the court orders it to be sealed, and that documents should be sealed only when necessary. Certain sealed filings in CM/ECF, however, contain sensitive non-public information that, if obtained without authorization and improperly released, could cause harm to the United States, the Federal Judiciary, litigants, and others.

**Your immediate action is needed to mitigate this apparent compromise and reduce the risk of future compromises of confidential court filings.** The Executive Committee considers it imperative that all courts make it a high priority to take the following steps to protect the security of certain highly confidential sealed filings

maintained in their court's electronic files in CM/ECF. The AO will provide guidance for implementing these new procedures, with input from the relevant advisory groups.

### **URGENT ACTION REQUIRED**

- To the extent they have not already done so, all courts should issue a standing or general order or adopt some other equivalent procedure requiring that highly sensitive documents (HSDs) will be accepted for filing only in paper form or via a secure electronic device. HSDs should be stored in a secure paper filing system or a secure standalone computer system that is not connected to any network, particularly the internet. The AO will provide courts with model language for a standing or general order as well as advice and guidance on how to establish and securely maintain a standalone computer system if a court chooses that option.
- This change in procedure should apply to all HSDs filed with the court. However, not every currently sealed filing should be considered an HSD; courts should use their discretion in determining which documents require HSD protection and thus should not reside on CM/ECF and which may continue to be entered into CM/ECF using that court's current sealing practices. Pleadings such as Title III applications and search warrants initially should be considered HSDs. Courts are cautioned not to be overinclusive in determining what is an HSD, as many pleadings currently filed under seal in CM/ECF do not merit the heightened protections addressed in this notice. For example, most documents similar to and including presentence reports, pretrial release reports, pleadings related to cooperation in most criminal cases, social security records, administrative immigration records, and sealed filings in many civil cases likely would not be sufficiently sensitive to require HSD treatment and could continue to be sealed in CM/ECF as necessary. Each court's standing or general order or equivalent procedure should address the types of filings it does and does not consider to be HSDs.
- Accompanying public docket entries for HSDs should not include personal or other identifying details related to those HSDs.
- Sealed court orders and any other sealed documents generated by the court pertaining to HSDs should not be uploaded into CM/ECF or the Public Access to Court Electronic Records (PACER) system or into any other system connected to a network or the internet, but must instead be transmitted to parties by a secure means specified by the court. The AO will provide further guidance regarding such transmissions.
- With respect to filings pertaining to highly sensitive information previously filed in CM/ECF, litigants may request that such sealed cases, matters, or filings be

removed from CM/ECF expeditiously. The manner in which parties may make such a request should be included in your standing or general order. The court should file and retain materials that are removed from CM/ECF in a secure paper filing system or standalone computer as described above.

The Executive Committee fully appreciates the practical implications of taking these steps and the administrative burden this will place on courts. Yet, it has determined that any such burdens are outweighed by the need to preserve the confidentiality of sealed filings that are at risk of compromise. The Federal Judiciary's foremost concern must be the integrity of and public trust in the operation and the administration of its courts.

cc: Circuit Executives  
District Court Executives  
Clerks, United States Courts