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

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

CITY'S POST-HEARING BRIEF

The Defendant, the City of Memphis ("the City"), respectfully submits this Post-Hearing Brief following the video hearing held on May 14, 2020 ("May 14 Hearing") to address the question of whether the City is out of compliance with Sanction 5 of the Court's October 29, 2018 Order Memorializing Sanctions. (*See* ECF No. 316.)

Sanction 5 of the Court's Order Memorializing Sanctions requires that:

> The City must 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.

(ECF No. 152, PageID 6289.)

Since entry of the Court's Order Memorializing Sanctions, the City has submitted six sets of search terms pursuant to Sanction No. 5. (*See* ECF Nos. 183, 199, 214, 239, 275, and 308.) The City has reported the search terms from the following units of the Memphis Police Department ("MPD"): Office of Homeland Security, Real Time Crime Center, General Investigative Unit, Homicide, Sex Crimes Unit and members of Command Staff. (*See, e.g.*, ECF No. 214, PageID

7311.) In each instance, the City clearly stated which units were being reported and included in the search term list. The city has reported a total of 14,432 search terms from the officers in those units, or approximately 2,400 search terms per quarter.

The City did not include the search terms of the "rank and file" MPD patrol officers in its quarterly submissions, or the search terms from the officers from the Organized Crime Unit ("OCU"), Multi-Agency Gang Unit ("MGU"), or the Internet Crimes Against Children ("ICAC") divisions.

During the May 14, 2020 Hearing, the City argued, *inter alia*, that it did not report the search terms of every "rank and file" patrol officer because it was overly burdensome to do so. (Hearing Tr., ECF No. 318, PageID 9368.) The City also argued that the social media accounts used by the officers are not operated or maintained by the MPD, and all search term reporting by MPD officers is necessarily voluntary. (*Id.*)

The Court invited the parties to submit briefing on the additional issues that were raised during the May 14 Hearing. (*Id.* at PageID 9369.) Accordingly, the City states as follows: [1]

I. The social media accounts used by MPD officers in the course of their law enforcement work are not MPD-sponsored or operated accounts.

First, it appears worthwhile to explain the City's understanding of the term "social media" and the ways in which individuals can use and "search social media" platforms. Generally, social media is defined as "forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos)." *Social Media,* Merriam-Webster (online

[1] The City additionally adopts and incorporates all arguments contained in its Pre-Hearing Brief (EFC No. 297).

edition).[2] Some commonly known examples of social media platforms include Facebook, Twitter, Instagram, TikTok, Vine, Pinterest, SnapChat, etc.[3] Subscriptions to these platforms are free, and registering for an account is generally easy, often requiring only an email address or mobile number to sign up. Most social media platforms also are accessible via an application, or "app", allowing account holders to download the app on their mobile devices. (Crowe Decl. ¶¶ 3, 4, attached as Exhibit A.)

As part of the signing-up process, the user creates a log-in and password for that account for future access. Accounts on social media platforms are not device-specific. A user can sign-on to his or her account on any device, *i.e.*, a computer or mobile device, that has access to the Internet, using either that particular social media platform's website or app. In each of these platforms, there is a mechanism to search for key words, such as other users' names or other posts of interests, like "Memphis Grizzlies." However, each of these social media platforms usually have their own form of search history control settings. For example, a user on Facebook can clear all search history. And while the user with the password can customize his or her own account, the social media platform creator has total control of the website or app. For example, Facebook can collect information from account users, but any third-party, such as the government, would have to issue a warrant for Facebook to provide that information. (Crowe Decl. ¶¶ 5-10.)

II. The social media accounts used by MPD officers in the course of their law enforcement work are not MPD-sponsored or operated accounts.

MPD has only four "official" MPD-sponsored social media accounts which it uses for

[2] https://www.merriam-webster.com/dictionary/social%20media
[3] In contrast, search engines such as Google or Yahoo do not require an account and do not fall into the category of social media.

communication to the public. MPD's official MPD-sponsored and operated Facebook account is "Memphis Police Department est.1827 @1827." Similarly, MPD operates an "official" MPD-sponsored and operated Twitter account with the following handle: @MEM_PoliceDept; an Instagram account at "Memphispolicedept;" and a NextDoor account at "Memphis Police Department." (Saleem Decl. ¶¶ 4-6, attached as Exhibit B.) The only officers with access to these accounts are officers assigned to the Public Information Office.[4] (Saleem Decl. ¶ 7.)

None of those accounts are used for investigatory purposes, but rather as avenues of communication to the public. (Crowe Decl. ¶ 11.)

Because MPD does not have any MPD-sponsored social media accounts for use in investigations, an officer who wishes to use a social media account in connection with her duties must necessarily use a social media account created by the officer to conduct social media investigations. (Crowe Decl. ¶ 12.) An MPD officer may choose to use his or her own personal social media account for use in investigation, or the officer may choose to create a second social media account that does not reveal that officer's identity or identify that officer as affiliated with the MPD. (Crowe Decl. ¶ 13.)[5] In both instances, the log-in and password are created by the officer. A social media account is not tied to or linked with any particular electronic device (such as a computer or phone), and it can be accessed on virtually any device with internet capabilities

[4] Those officers are: Lt. Karen Rudolph, Sgt. William Kaiser, Officer Louis Brownlee, PST Braulio Hernandez, and PST Corey Douglas.

[5] It is very common for a person to have multiple accounts on social media platforms. For example, Facebook estimates that fake accounts represented approximately 5% of its 2.6 Billion worldwide monthly active users during Q4 2019 and Q1 2020. *See* https://transparency.facebook.com/community-standards-enforcement#fake-accounts; https://investor.fb.com/investor-news/press-release-details/2020/Facebook-Reports-First-Quarter-2020-Results/default.aspx; https://www.latimes.com/business/technology/story/2019-11-18/facebooks-massive-fake-numbers-problem

if the log-in and password are known. (Crowe Decl. ¶ 14.)

Major Darren Goods testified regarding the need to use undercover or "UC accounts" to perform criminal investigations.

> We do have officers that have what we call UC accounts. It's pretty much accounts that they've created. They've taken on a persona of another name or street name or moniker, and they use those accounts to conduct these searches -- to conduct the search terms. And the reason why is because, first of all, they don't want -- they're trying to maintain their own personal safety and integrity. Because they don't want to be searching Trulla Mafia or -- which is one of the most violent gangs we're dealing with now. And then have a Trulla Mafia member find out that, hey, Darren Goods has been searching for me. And then it's a matter of just simply, you know, Googling Darren Goods and you can find, you know, my social media page and all my friends and families and that kind of exposes my friends and families to some type of retaliatory attacks and that sort of thing. So that's the primary reason why they use what we call the UC accounts, undercover accounts, to actually run those searches when they're involved in their respective investigations.

(Hearing Tr., ECF No. 318, PageID 9355-56.)

With both types of accounts, the officers' personal accounts and undercover accounts created by the officers for use if needed for investigations, control over the accounts is maintained exclusively by the MPD officer who created the account. (Crowe Decl. ¶ 15.) The officer creates the username and password for the account, and that officer controls who has access to that log-in information. (Hearing Tr., ECF No. 318, PageID 9357.)

III. It is impossible for the City to electronically collect the search terms from its officers' social media accounts.

The City does not have the ability to access or monitor any officer's individual social media account. Even when using a City-owned electronic device or via the City's network, an officer must first log-in to the social media platform using the login information he or she created. The City does not have access to their log-in information and cannot simply log-on to the various accounts to collect the search terms used by the officers during investigations. (Boateng Decl. ¶¶

8, 10, attached as Exhibit C.)

Moreover, any activity the officer conducts while logged-in to the social media platform is not discernable or discoverable by the City's Information Services department or MPD. (Boateng Decl. ¶ 8, 9; Crowe Decl. ¶ 15.) This includes the search terms an officer enters into the search bar of the social media platform. (Boateng Decl. ¶ 8, 9.)

Thus, even if the officer is accessing his or her social media account from a City-owned electronic device or accessing the social media account via the City's network, the City has no technical ability to electronically "audit" what search terms the officer uses while "inside" the social media platform. (Boateng Decl. ¶ 8, 9.)

Accordingly, the only way for the City to acquire the search terms used by the officers in order to report them to the Court is to demand that the officers self-report the search terms used in the course of their police work. There is no way to determine the accuracy of the officers' submissions.

IV. It would be overly burdensome to collect the search terms of every MPD officer and employee, when weighed against the impracticability of the exercise.

MPD currently has approximately 2,065 sworn officers and 1,090 non-sworn employees. (Saleem Decl. ¶ 3.) To collect search terms from over 3,100 persons would be unduly burdensome. In theory, the MPD could require each officer and employee to provide their search terms via email, likely at the end of their shift, which would result in receipt of approximately 1,600 to 2,000 emails over every 24-hour period, depending on how many officers are on duty. Each email would have to be read, whether search terms were used or not.[6]

[6] The City notes that the search terms collected from patrol officers are unlike the search terms used by officers in the investigative bureaus, and those search terms are very unlikely to relate to First Amendment activity due to the nature of patrol officers' police work.

Additionally, MPD would have to track which officers or employee reported terms and those who did not, follow-up with the persons who failed to report, and then report the terms it was able to collect. Moreover, because the officer maintains exclusive control over the social media accounts he or she may use for investigations, the officer alone would know what terms he or she actually used in her role as a police officer as opposed to those used in personal and social inquiries unrelated to her job.

Importantly, any action by MPD to search the social media of the officer or employee without a warrant would implicate the officer's Fourth Amendment rights. Absent a warrant to search the officer's mobile phone or a subpoena of the social media platform's records, the City has no way of auditing the officer's social media search history to ensure that the officer actually reported every reportable search term. It is well-settled that the Fourth Amendment "'guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government,' without regard to whether the government actor is investigating crime or performing another function." *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 755–56, 130 S. Ct. 2619, 2627–28, 177 L. Ed. 2d 216 (2010) (emphasis added) (quoting *Skinner v. Railway Labor Executives' Assn.,* 489 U.S. 602, 613–614, 109 S.Ct. 1402, 103 L.Ed.2d 639 (1989)). "The Fourth Amendment applies as well when the Government acts in its capacity as an employer." *Id.* (quoting *Treasury Employees v. Von Raab,* 489 U.S. 656, 665, 109 S.Ct. 1384, 103 L.Ed.2d 685 (1989)). Moreover, [i]ndividuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer." *O'Connor v. Ortega*, 480 U.S. 709, 717, 107 S. Ct. 1492, 1497, 94 L. Ed. 2d 714 (1987).

"Searches and seizures by government employers or supervisors of the private property of their employees . . . are subject to the restraints of the Fourth Amendment." *O'Connor v. Ortega*,

480 U.S. 709, 715, 107 S. Ct. 1492, 1496, 94 L. Ed. 2d 714 (1987). The *O'Connor* Court explained:

> Not everything that passes through the confines of the business address can be considered part of the workplace context, however. An employee may bring closed luggage to the office prior to leaving on a trip, or a handbag or briefcase each workday. While whatever expectation of privacy the employee has in the existence and the outward appearance of the luggage is affected by its presence in the workplace, the employee's expectation of privacy in the *contents* of the luggage is not affected in the same way. The appropriate standard for a workplace search does not necessarily apply to a piece of closed personal luggage, a handbag or a briefcase that happens to be within the employer's business address.

Id. at 1497.

Additionally the Supreme Court has determined that a person has a significant Fourth Amendment privacy interest in the contents of his or her mobile phone. *See Riley v. California*, 573 U.S. 373, 403, 134 S. Ct. 2473, 2494–95, 189 L. Ed. 2d 430 (2014) (holding that police must get a warrant before searching a cell phone, even one seized incident to arrest).

Here, an MPD officer has a reasonable expectation of privacy in his or her privately-owned cell phones and/or personally-created social media accounts contained therein, even when the phone and/or the social media accounts are used at the workplace. A search of that officer's social media account or seizure of the officer's personal cell phone would be subject to the restraints of the Fourth Amendment.

In short, neither MPD nor the City Information System's department, has a mechanism, absent a warrant, to compel its officers to turn over their social media data or search histories. MPD can, and does, ask certain officers who routinely "collect" information on social media to report the search terms they used during the course of their investigations, but MPD has no way of determining if the terms reported are accurate or complete when do we do this.

Moreover, in the case of patrol officers, the terms used in their social media searches would not represent an effort to "collect" information on social media but are more akin to the historical pre-internet actions of patrol officers walking a beat and asking questions to gain information relevant to solving or preventing crime.

To be clear, the City stands ready to demand that all 3,100+ officers and employees submit their search terms, just as it has done for the officers assigned to the various investigative units for which it has been reporting search terms from over the past 18 months. In the absence of the ability to audit an officer's personal social media account, however, the accuracy of the reporting is dependent upon each individual officer's efforts and accuracy in compiling the terms.

Accordingly, and respectfully, the search term reporting requirement of Sanction 5 request is impracticable and largely futile when weighed against the huge administrative burden this ongoing task will impose on the City's limited resources.

CONCLUSION

The City understands the need for transparency with its officers' use of social media, but asks the Court, respectfully, to reconsider Sanction 5 in view of the reality of the impracticability of the endeavor.

Respectfully Submitted,

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

s/ Bruce McMullen
Bruce McMullen (#18126)
R. Mark Glover (#6807)
Jennie Vee Silk (#35319)
Mary Wu Tullis (#31339)

165 Madison Avenue, Suite 2000
Memphis, Tennessee 38103
Telephone (901) 526-2000
E-mail: bmcmullen@bakerdonelson.com
mglover@bakerdonelson.com
jsilk@bakerdonelson.com
mtullis@bakerdonelson.com

Attorneys for Defendant, The City of Memphis

CERTIFICATE OF SERVICE

I hereby certify that on the 21st day of May 2020, a copy of the attached pleading was filed electronically. Notice of this filing will be served by operation of the Court's electronic filing system to all counsel of record.

Thomas H. Castelli
ACLU Tennessee, Inc.
P.O. Box 120160
Nashville, TN 37212
tcastelli@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
Bruce McMullen

EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TENNESSEE
WESTERN SECTION

ACLU OF TENNESSEE, INC.,

Plaintiffs,

vs. 2:17-cv-2120-JPM-jay

CITY OF MEMPHIS, TENNESSEE

Defendants.

DECLARATION OF DON CROWE

In accordance with the provisions of 28 U.S.C. § 1746, the undersigned, Don Crowe, does hereby make the following declaration pertinent to the above-styled cause of action:

1. I am the Deputy Chief of Information Technology for the Memphis Police Department.

2. As a part of my duties, I am generally familiar with the Memphis Police Department's use of social media websites and applications. In that regard, I am aware of the functionalities of certain social media websites and applications, like Facebook, Instagram, Snap and other similar social media platforms.

3. Subscriptions to social media platforms like, Facebook, Twitter, Instagram, TikTok, Vine, Pinterest, SnapChat, etc. are free, and registering for an account is generally easy, often requiring only an email address or mobile number to sign up.

4. Most social media platforms also are accessible via an application, or "app", allowing account holders to download the app on their mobile devices.

5. As part of the signing-up process, the user creates a password for that account for future access.

6. Accounts on social media platforms are not device-specific.

7. A user can sign-on to his or her account on any device, *i.e.*, a computer or mobile device, that has access to the Internet, using either that particular social media platform's website or app.

8. In each of these platforms, there is a mechanism to search for key words, such as other users' names or other posts of interests.

9. Each of these social media platforms usually have their own form of search history control settings; for example, a user on Facebook can clear all search history.

10. The user with the password can customize his or her own account, and the social media platform creator has total control of the website or app. For example, Facebook can collect information from account users, but any third-party, such as the government, would have to issue a warrant for Facebook to provide that information.

11. None of the four "official" MPD-sponsored social media accounts which it uses for communication to the public are used for investigatory purposes.

12. Because MPD does not have any MPD-sponsored social media accounts for use in investigations, an officer who wishes to use a social media account in connection with her duties must necessarily use a social media account created by the officer to conduct social media investigations.

13. An MPD officer may choose to use his or her own personal social media account for use in investigation, or the officer may choose to create a second social media account that does not reveal that officer's identity or identify that officer as affiliated with the MPD.

14. A social media account is not tied to or linked with any particular electronic device (such as a computer or phone), and it can be accessed on virtually any device with internet capabilities if the log-in and password are known.

15. Control over any social media accounts is maintained exclusively by the MPD officer who created the account.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed this 21st day of May, 2020.

D. E. Crowe 5-21-20

Don Crowe

EXHIBIT B

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TENNESSEE
WESTERN SECTION

ACLU OF TENNESSEE, INC.,

Plaintiffs,

vs. 2:17-cv-2120-JPM-jay

CITY OF MEMPHIS, TENNESSEE

Defendants.

DECLARATION OF ZAYID A. SALEEM

In accordance with the provisions of 28 U.S.C. § 1746, the undersigned, Zayid A. Saleem, does hereby make the following declaration pertinent to the above-styled cause of action:

1. I am the Legal Advisor to the Memphis Police Department.

2. As a part of my duties, I am generally familiar with the Memphis Police Department's operations and use of social media websites and applications.

3. MPD currently has approximately 2,065 sworn officers and 1,090 non-sworn employees.

4. MPD has four "official" MPD-sponsored social media accounts which it uses for communication to the public.

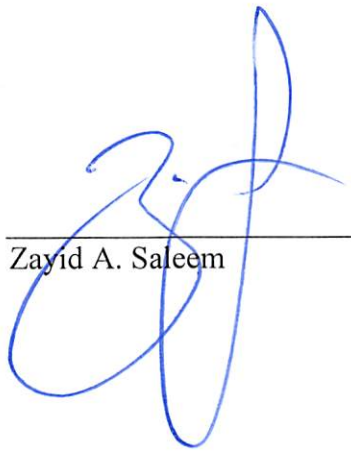
5. MPD's official MPD-sponsored and operated Facebook account is "Memphis Police Department est.1827 @1827."

6. MPD operates an "official" MPD-sponsored and operated Twitter account with the following handle: @MEM_PoliceDept; an Instagram account at "Memphispolicedept;" and a NextDoor account at "Memphis Police Department."

7. The only officers with access to these accounts are officers assigned to the Public Information Office: Lt. Karen Rudolph, Sgt. William Kaiser, Officer Louis Brownlee, PST Braulio Hernandez, and PST Corey Douglas.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed this 21st day of May, 2020.



Zayid A. Saleem

EXHIBIT C

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TENNESSEE
WESTERN SECTION

ACLU OF TENNESSEE, INC.,

Plaintiffs,

vs. 2:17-cv-2120-JPM-jay

CITY OF MEMPHIS, TENNESSEE

Defendants.

DECLARATION OF AUGUSTINE BOATENG

In accordance with the provisions of 28 U.S.C. § 1746, the undersigned, Augustine Boateng, does hereby make the following declaration pertinent to the above-styled cause of action:

1. I am the Information Security Manager for the City of Memphis, Tennessee.

2. As a part of my duties, I am familiar with the Information Systems of the City of Memphis. In that regard, I am aware of the capabilities and limitations of the City's access to employees' personal information contained in an individual's Facebook, Instagram, Snap and similar social media accounts.

3. All social media websites and applications leverage advance encryption to protect any form of data leak to any unauthorized user or system. The City would be considered an unauthorized user or system.

4. The City currently has the technological capabilities to view in the aggregate what type of applications users access with City computers and what times the application was accessed.

5. In order to determine which City computer was used to view the application, the City would have to query gigabytes of aggregated data across multiple systems.

6. Upon a successful query, the City will only be able to determine what application was accessed by the computer and what time the transaction took place.

7. The City does not have the technological capabilities to view what applications users access with devices that are not connected to the City's network (Wireless or Wired) or monitored with any of the City's systems, including personal cell phones and City-issued cell phones.

8. Once the user authenticates into a secured application, *i.e.*, Facebook, Instagram, Snapchat, etc., the City has no way of monitoring or accessing any transactions that are performed in that application, such as any postings, comments, likes or searches or search terms.

9. In other words, the City may be able to determine that a City computer was used to access Facebook, but the City is not capable of determining which Facebook account was accessed, much less what activity occurred on the Facebook account.

10. None of the data would be available to the City without the employee's permission, which must be given in writing.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed this 21st day of May, 2020.

Augustine Boateng

Augustine Boateng