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.	)	

SEALED MOTION FOR IMMEDIATE MODIFICATION OF THE KENDRICK CONSENT DECREE

The Defendant, the City of Memphis ("the City"), pursuant to Fed. R. Civ. P. 60(b)(5) and (6), moves for immediate relief from Section I of the September 14, 1978 Order, Judgment and Decree entered in the case of *Kendrick, et al v. Chandler, et al*, No. 2:76-cv-00449 (W.D. Tenn. 1978) (the "Consent Decree") (*See* Consent Decree, ECF 9-1).

Prospective application of Section I of the Decree is inequitable because a significant change in factual conditions and in law renders continued enforcement detrimental to the public interest. Moreover, the law surrounding government surveillance and First Amendment rights has been clarified since the entry of the Decree. Most importantly, however, is that the Decree, as interpreted by the Monitor, impinges upon legitimate law enforcement interests in such a way that the continued enforcement of the Consent Decree is now detrimental to public safety, and therefore inequitable.

For these reasons and those set forth in the accompanying Memorandum of Law, the City of Memphis respectfully requests that the Court vacate or significantly modify Section I of the Consent Decree.

Respectfully Submitted,

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

s/ Jennie Silk

Buckner Wellford (#9687)
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: bwellford@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 25th day of September 2019, 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
Mandy Floyd
ACLU Tennessee, Inc.
P.O. Box 120160
Nashville, TN 37212
tcastelli@aclu-tn.org

Attorneys for Intervening Plaintiff

s/ Jennie Silk
Jennie Silk

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

SEALED MEMORANDUM OF LAW IN SUPPORT OF MOTION FOR IMMEDIATE MODIFICATION OF THE KENDRICK CONSENT DECREE

I. BACKGROUND AND PROCEDURAL HISTORY

In 1976 a group of plaintiffs brought a civil action for declaratory and injunctive relief against the City of Memphis ("the City") in *Kendrick, et al v. Chandler, et al*, No. 2:76-cv-00449 (W.D. Tenn. 1978). The *Kendrick* plaintiffs alleged, *inter alia*, that the Memphis Police Department ("MPD") investigated and maintained files on persons engaged in non-criminal, constitutionally protected First Amendment activities. (*Kendrick* Comp. ¶ 7, ECF No. 33-1). The *Kendrick* plaintiffs claimed this conduct on the part of MPD had a chilling effect upon their First Amendment rights. *Id.* at ¶ 16.

On September 14, 1978, the Court entered a Consent Order and Decree (the "Consent Decree") in *Kendrick, et al v. Chandler, et al*, No. 2:76-cv-00449 (W.D. Tenn. 1978). (*See* Consent Decree, ECF No. 151, PageIDs 6280-86). The Consent Decree prohibited the City of Memphis "from engaging in law enforcement activities which interfere with any person's rights protected by the First Amendment to the United States Constitution including, but not limited to, the rights to communicate an idea or belief, to speak and dissent freely, to write and to publish, and to associate privately and publicly for any lawful purpose." (ECF No. 151, PageID 6281).

The provisions of the Consent Decree were directly at issue in the underlying litigation in this case.

In an Order entered August 10, 2018 (ECF No. 120) the Court granted summary judgment in part to the Intervening Plaintiff, the American Civil Liberties Union of Tennessee, Inc. ("ACLU-TN"), finding that the City had violated the Consent Decree in several respects. (ECF No. 120 at PageIDs 4880-4882, 4886). The Court also, however, observed that in the event that the Consent Decree "is outdated due to a change in legal or other circumstances, the City is free to file a motion to modify the Consent Decree." *Id.* at 4877. The Court noted that the City intimated its intention, if necessary, to file a Motion under Fed. R. Civ. P. 60(b) to do just that. *Id.* at 4877.

On August 16, 2018, the City filed a Motion for Relief from Judgment or Order and accompanying Memorandum of Law in Support of Motion to Modify and/or Vacate Judgment. ("Motion to Modify") (ECF No. 124).

After a trial on the merits, the Court found the City in contempt of additional portions of the Consent Decree. S*ee* October 26, 2018 Opinion and Order (ECF No. 151) ("October 26, 2018 Order"). The Court imposed five sanctions against the City "[t]o ensure compliance with the Consent Decree generally, and especially with the requirement that the City familiarize its officers with the contents of the Decree." (ECF No. 152). In addition to those sanctions, the Court ruled that it would appoint an independent monitor "to supervise the implementation of the sanctions described above." *Id.* at PageID 6290.

On November 14, 2018, the Court entered an Order Setting Consent Decree Modification Schedule and Setting Public Comment Period. (ECF 159). After consultation with the Intervening Plaintiff, and after reviewing the October 26, 2018 Order, the City concluded that its

broad Motion to Modify was premature in that it would present hypotheticals rather than existing facts. Moreover, the City determined any modification of the Consent Decree would be best addressed after a period of attempted compliance with the Consent Decree, and after a period of operation under the supervision and oversight associated with the then soon-to-be Court-appointed monitor. Once the City operated in that manner for a period of time, the City intended to revisit its Motion to Modify, if necessary. The Parties further agreed that they could make progress on proposed joint modifications to the Consent Decree if they had additional time to collaborate with each other and the Monitor. *See* Joint Motion to Stay the City's Motion to Modify and/or Vacate Judgement (ECF No. 175, PageID 6523).

On December 31, 2018, the Court granted the Joint Motion to Stay the City's Motion to Modify and/or Vacate Judgment, staying proceedings on the City's Motion to Modify until January 2, 2020. (ECF No. 178, PageID 6545). The Court noted, however, that it may "order that discovery and modification proceedings resume if 'either party in good faith believes that the collaborative attempt to suggest Consent Decree modifications has reached an impasse.'" (ECF No. 174 at PageID 6527.)

Since that time, the City has worked diligently to comply with the Court's sanctions in the Order, as well as to work with the Court-appointed Monitor and the ACLU-TN to revise its policies and procedures. A series of recent interpretations of the Consent Decree by the Independent Monitor, however, has left the City no choice but to seek immediate modification or clarification of Section I of the Consent Decree in the interest of maintaining public safety.

Accordingly, the City now moves, pursuant to Rule 60(b)(5) of the Federal Rules of Civil Procedure, to modify the Decree by vacating or significantly modifying Section I of the Decree, as interpreted by the Monitor, because it unduly burdens legitimate investigative activities and

creates restrictions that are unnecessary for the protection of First Amendment rights.[1]

Section I of the Consent Decree states:

> Restrictions on Joint Operations
>
> The defendants and the City of Memphis shall not encourage, cooperate with, delegate, employ or contract with, or act at the behest of, any local, state, federal or private agency, or any person, to plan or conduct any investigation, activity or conduct prohibited by this Decree.

Consent Decree, Section I (ECF No. 151, PageID 6284).

The City has interpreted this Section to prohibit it from using other agencies or persons as "surrogates" to do indirectly what it could not do directly. As explained below, the Monitor's reading of Section I, however, prevents inter-agency law enforcement information-sharing and cooperation.

Section I should be modified because it does not directly protect any federal right. Moreover, the law and circumstances surrounding surveillance and the First Amendment have changed significantly since the time of the original *Kendrick* lawsuit. Additionally, the City has complied with the Consent Decree to the best of its ability since the Court found it in contempt, and it will continue to cooperate with the Independent Monitor concerning its ongoing compliance with other portions of the Consent Decree.

Most importantly, Section I should be modified or vacated because, as interpreted, it creates an undue burden on law enforcement. By prohibiting joint operations with other law enforcement agencies, Section I inhibits investigations of terrorism, hate crimes, bombings, gang crimes, sex crimes against children, and mass shootings that by their very nature, require open sharing of information across local, state, and federal law enforcement agencies.

[1] The instant Motion relates only to modification of Section I of the Consent Decree, but the City does not waive its right to modify other provisions of the Consent Decree at a later date.

Additionally and separately, the City requests an *in camera* meeting with the Court and the Parties to discuss an extremely sensitive law enforcement matter at the Court's earliest convenience.

II. LAW AND ARGUMENT

A. Applicable Legal Standard

"Consent decrees are not 'entitlements.'" *John B. v. Emkes*, 710 F.3d 394, 398 (6th Cir. 2013). Instead, a decree may remain in force only so long as it continues to remedy a violation of federal law." *Id.*

A consent decree is subject to a Rule 60(b) motion because it is "a judicial decree that is subject to the rules generally applicable to other judgments and decrees." *Rufo v. Inmates of Suffolk Cnty. Jail*, 502 U.S. 367, 378 (1992). Accordingly, a district court may grant relief under Rule 60(b)(5) if "among other things, 'applying [the judgment or order] prospectively is no longer equitable.'" *Horne v. Flores*, 557 U.S. 433, 447 (2009).

Rule 60(b)(5) "provides a means by which a party can ask a court to modify or vacate a judgment or order if 'a significant change either in factual conditions or in law' renders continued enforcement 'detrimental to the public interest.'" *Id.* (quoting *Rufo v. Inmates of Suffolk County Jail*, 502 U.S. 367, 384 (1992)). The party seeking relief bears the burden of establishing that changed circumstances warrant relief, but once a party carries this burden, a court abuses its discretion when it refuses to modify an injunction or consent decree in light of such changes. *Id.* (citations and quotations omitted).

Modification of a consent decree is appropriate: (1) "when changed factual conditions make compliance with the decree substantially more onerous," (2) "when a decree proves to be unworkable because of unforeseen obstacles," or (3) "when enforcement of the decree without modification would be detrimental to the public interest." *United States v. State of Mich.*, 62 F.3d

1418 (6th Cir. 1995). Rule 60(b)(5) "does not allow modification simply 'when it is no longer convenient to live with the terms of a consent decree,' but solely when there is 'a significant change either in factual conditions or in law.'" *Northridge Church v. Charter Twp. of Plymouth*, 647 F.3d 606, 613-14 (6th Cir. 2011) (quoting *Rufo*, 502 U.S. at 383–84). The party seeking to show such a change exists "bears the burden of establishing that a significant change in circumstances warrants revision of the decree." *Id.* at 614. If that party carries its burden, then the district court "should consider whether the proposed modification is suitably tailored to the changed circumstance." *Id.*

Rule 60(b)(5) serves a particularly important function in "institutional reform litigation." *Horne*, 557 U.S. at 447. "[I]njunctions issued in such cases often remain in force for many years, and the passage of time frequently brings about changed circumstances—changes in the nature of the underlying problem, changes in governing law or its interpretation by the courts, and new policy insights—that warrant reexamination of the original judgment." *Id.*

Horne recognized that institutional reform decrees require courts to take a "flexible approach" to Rule 60(b)(5) motions addressing such decrees. *Id.* at 450.

> A flexible approach allows courts to ensure that responsibility for discharging the State's obligations is returned promptly to the State and its officials when the circumstances warrant. In applying this flexible approach, courts must remain attentive to the fact that federal-court decrees exceed appropriate limits if they are aimed at eliminating a condition that does not violate federal law or does not flow from such a violation. If a federal consent decree is not limited to reasonable and necessary implementations of federal law, it may improperly deprive future officials of their designated legislative and executive powers.
>
> *Id.* (internal citations omitted)

The Court also noted that "institutional reform injunctions often raise sensitive federalism concerns." *Id*. The *Horne* Court stated that its flexible approach "allows a court to recognize that the longer an injunction or consent decree stays in place, the greater the risk that it will improperly interfere with a State's democratic process." *Id*. at 453.

The Sixth Circuit established the following two-prong test in applying this flexible approach:

> First, whether the State has achieved compliance with the federal-law provisions whose violation the decree sought to remedy and second, whether the State would continue that compliance in the absence of continued judicial supervision.

Emkes, 710 F.3d at 412 (citations omitted).

Accordingly, the City seeks modification of the Decree under Federal Rule of Civil Procedure 60(b)(5). The rule provides in pertinent part:

> On motion and upon such terms as are just, the court may relieve a party or a party's legal representative from a final judgment, order, or proceeding for the following reasons: . . . (5) the judgment has been satisfied, released, or discharged, or a prior judgment upon which it is based has been reversed or otherwise vacated, or it is no longer equitable that the judgment should have prospective application . . . .

Fed. R. Civ. P. 60(b) (5).

B. Argument

Here, prospective application of Section I of the Decree is inequitable because a significant change in factual conditions and in law renders continued enforcement detrimental to the public interest. The Consent Decree does not secure a federal right and the law surrounding government surveillance and First Amendment rights has been clarified since the entry of the Decree. Most importantly, however, is that the Decree, as interpreted by the Monitor, impinges upon legitimate law enforcement interests in such a way that the continued enforcement of the Consent Decree is now detrimental to public safety, and therefore inequitable.

1. A change in the law warrants modification of a consent decree.

"There is … no dispute but that a sound judicial discretion may call for the modification of the terms of an injunctive decree if the circumstances, whether of law or fact, obtaining at the time of its issuance have changed, or new ones have since arisen." *Rufo*, 502 U.S. at 380

(quoting *Sys. Fed'n No. 91, Ry. Emp. Dep't, AFL-CIO v. Wright*, 364 U.S. 642, 647 (1961)). Such "changed circumstances" warranting revision include changes in the statutory or decisional law supporting entry of the original decree. *See Railway Employees v. Wright*, 364 U.S. 642, 650 (1961) (holding that modification of consent decree was appropriate where statutory amendment made clear that prohibitions in decree were no longer illegal). In particular, "modification of a consent decree may be warranted when the statutory or decisional law has changed to make legal what the decree was designed to prevent." *Rufo*, 502 U.S. at 388. Stated another way, a court should grant relief under Rule 60(b)(5) where the federal claim underlying the decree, though valid when entered, is no longer supported by federal law. *See Evans v. City of Chicago*, 10 F.3d 474 (7th Cir. 1993) (en banc), *cert. denied*, 114 S. Ct. 1831 (1994).

Here, such a change in law exists that warrants modification of the *Kendrick* Consent Decree. In 1983, the Sixth Circuit, interpreting *Laird v. Tatum*, 408 U.S. 1 (1972), for the first time, held that if an undercover investigation or surveillance is conducted in good faith and is not designed to regulate or constrain a person or group's First Amendment activities, then that investigation or surveillance does not violate First Amendment rights, even though the investigation or surveillance may be targeted at a particular socio-political group or at the group's First Amendment activities. *See Gordon v. Warren Consol. Bd. of Educ.*, 706 F.2d 778, 781 (6th Cir. 1983).

In *Gordon*, the plaintiffs were high school teachers and students in Michigan. During the 1977-78 school year, school officials helped place an undercover policewoman in two classes at the school for the purpose of investigating drug trafficking at the school. *Id.* at 778. The undercover officer was placed in classes with teachers who had "liberal reputations." *Id.* at 779.

During her undercover investigation, the officer uncovered no evidence of drug sales occurring at the high school. A few months after the termination of the surveillance, several students learned of the undercover policewoman's true identity and learned of the drug surveillance operation. Disclosure of the investigation allegedly dramatically altered the content and open discussion methodology that had characterized the psychology and sociology classes targeted by the undercover officer. Class discussions allegedly became stilled, and certain topics were avoided, and students refused to freely express their opinions. *Id.*

The teachers and students filed a § 1983 suit against the school system alleging that the teachers' political beliefs motivated school officials to target the surveillance towards the teachers' particular classrooms. *Id.* at 780. They further alleged that the surveillance chilled their speech. *Id.* The district court dismissed the complaint because the complaint alleged nothing more than a subjective chilling of the plaintiffs' First Amendment rights and the Sixth Circuit agreed. *Id.*

First, the Sixth Circuit noted that *Laird v. Tatum* controlled the case stating:

> In *Laird* the complaint alleged that the United States Armed Forces intelligence agencies had engaged in the surveillance of lawful and peaceful civilian activity, collected information on political protests which served no legitimate military purpose, and disseminated this information to various military headquarters in the United States. These activities allegedly curtailed plaintiff's First Amendment rights and deprived them of their constitutionally guaranteed right of privacy. The Supreme Court rejected the claims that the intelligence activities had a "chilling effect" upon the exercise of First Amendment rights because plaintiffs were unable to point to any resulting direct injury or immediate threat of harm. The mere existence of a military data-gathering system does not constitute a justiciable controversy. "Allegations of subjective chill are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm; the federal courts established pursuant to Article III of the constitution do not render advisory opinions."

Gordon v. Warren Consol. Bd. of Educ., 706 F.2d 778, 780 (6th Cir. 1983) (quoting *Laird v. Tatum*, 408 U.S. 1, 13-14 (1972)) (emphasis added).

Accordingly, in *Gordon*, the Sixth Circuit found that the plaintiffs failed to allege that the covert operation resulted in any tangible consequence, but rather only a subjective chilling on plaintiff's speech. *Gordon*, 706 F.2d at 780-81. Furthermore, it did not matter that the investigation focused on particular socio-political groups. The court stated that "even accepting plaintiffs' assertion that the investigation focused on classes where students and teachers held 'liberal' socio-political views, there was no indication that the investigation had any tangible and concrete inhibitory effect on the expression of particular socio-political views in these classrooms." *Id.* at 781. The court found that the undercover investigation was made in good faith, and was prompted by the school officials' legitimate concern about possible illegal drug activity at the school. *Id.* As a result, the plaintiff's subjective fear that the content of class discussions might be reported to school administrators or others was insufficient to establish a First Amendment claim. *Id.*

Importantly, the *Gordon* Court clarified that surveillance targeting First Amendment activity as part of a good faith investigation is permissible so long as Fourth Amendment protections are observed.

> We find no support for plaintiff's suggestion that an undercover investigation is necessarily constitutionally infirm because the focus of that investigation was directed to classes where particular socio-political views were espoused. Courts have recognized that physical surveillance consistent with Fourth Amendment protections in connection with a good faith law enforcement investigation does not violate First Amendment rights, even though it may be directed at communicative or associative activities. Here there is no suggestion that the investigation of drug activities was conducted in bad faith and was surreptitiously designed to regulate or proscribe the content of discussion in the classroom. Furthermore, plaintiffs do not contend that the investigation invaded any legitimate expectation of privacy so as to invoke Fourth Amendment protections. Finally, it should also be noted that this case is distinguishable from those cases where an investigation significantly invades rights of associational privacy and is not germane to the detection of specific criminal conduct.

Id. at 781 n.3 (internal citations omitted) (emphasis added).

When *Kendrick* was being litigated in the mid-1970s, the law surrounding surveillance of First Amendment activity was in flux. *Laird* was decided in 1972, but it took several years for the lower courts to develop its holding as applied to various surveillance situations. In 1983, the Sixth Circuit finally interpreted *Laird* in *Gordon*, and foreclosed the possibility that a plaintiff could allege a First Amendment violation based upon law enforcement's good faith investigation or surveillance that did not have an objective chilling effect on speech.

Since *Gordon*, Courts in this Circuit and beyond continue to interpret *Laird* in the same manner as *Gordon, i.e.* that for surveillance to give rise to a constitutional violation, something more than a subjective chilling of speech is required. *See, e.g. Am. Civil Liberties Union v. Nat'l Sec. Agency*, 493 F.3d 644, 661 (6th Cir. 2007) (finding that plaintiffs lacked standing to bring a First Amendment claim because they failed to establish that they were regulated, constrained, or compelled directly by the government's actions, instead of by their own subjective chill); *Ghandi v. Police Dep't of City of Detroit*, 747 F.2d 338, 347 (6th Cir. 1984) (explaining that the government's use of informants does not by itself give rise to a constitutional violation); *Handschu v. Special Servs. Div.*, 475 F. Supp. 2d 331, 353–54 (S.D.N.Y. 2007), *order vacated on reconsideration on other grounds*, No. 71 CIV. 2203(CSH), 2007 WL 1711775 (S.D.N.Y. June 13, 2007) (holding that plaintiffs failed to bring a justiciable claim that NPYD chilled their First Amendment rights by photographing and videotaping a political march); *Fifth Ave. Peace Parade Comm. v. Gray*, 480 F.2d 326, 332-33 (2d Cir. 1973) (holding that FBI's investigation of a planned anti-war protest, including examination of bank and transportation records was a lawful exercise of the agency's duty to maintain public safety); *Donohoe v. Duling*, 465 F.2d 196, 199-202 (4th Cir. 1972) (explaining that photographic surveillance by police at political and religious events does not present justiciable claim of injury).

Gordon undermines many of the *Kendrick* Consent Decree's provisions. For example, the Consent Decree prohibits "Political Intelligence", defined as "the gathering, indexing, filing, maintenance, storage or dissemination of information, or any other investigative activity, relating to any person's beliefs, opinions, associations or other exercise of First Amendment rights." (ECF No. 151, PageID 6281.) More importantly for this Motion, Section I of the Consent Decree bars the City of Memphis from "cooperat[ing] with" any agency or person to "plan or conduct any investigation, activity or conduct prohibited by [the] Decree. *Id.* at PageID 6284.

While at the time this Court entered the Consent Decree the plaintiffs may have had a valid federal claim that investigations of them based upon their political statement violated their constitutional rights, any such claim could not be maintained in the present day following *Laird* and *Gordon*. Indeed, the *Kendrick* plaintiffs arguably would not even have standing to bring such a claim in the present day.

At the very least, the Sixth Circuit's decision in *Gordon* clarified a fundamental misunderstanding among the parties to the Decree, and upon which the Decree was based: that the City, by investigating First Amendment activity, had violated the U.S. Constitution. In short, it is now plainly legal to engage in much of the surveillance activity the Decree was designed to prevent, making continued enforcement of most aspects of the Decree inequitable under Fed. R. Civ. P. 60(b)(5).

Moreover, and more importantly for this Motion, Section I's restriction on cooperation is not required by the First Amendment or the U.S. Constitution. There is no constitutional right to be free from cooperation with local, state, and federal law enforcement agencies. Moreover, the Constitution does not require evidence of criminal conduct before law enforcement agencies may undertake investigations of individuals because of statements made by them. Because

Section I of the Decree is no longer supported by legitimate interests, and is severely hampering law enforcement activities which are otherwise legal, this Court may grant a modification of the Decree's provisions.

Because the Consent Decree's onerous restraints on police intelligence work have no basis in existing federal law and do not secure any federal right, the Decree should be modified to the extent herein requested.

2. Section I of the Consent Decree is unworkable and a detriment to public safety.

As will be illustrated *infra*, Section I of the Consent Decree should be modified because it is unworkable for a modern police force. In particular, that portion of the Consent Decree hampers the City's exercise of its legitimate law enforcement functions and requires the City to expend scarce resources to assure compliance with restrictions that go well beyond that which is required by federal law.

The burden that a consent decree imposes on state and local governments is properly considered under Rule 60(b)(5). The U.S. Supreme Court in *Rufo* expressly acknowledged that the effect of a decree on the consenting party plays an important role in a district court's assessment of the need for modification. While mere inconvenience would not warrant modification of a consent decree, the Court noted, revision can be necessary if changed circumstances "make compliance with the decree substantially more onerous." 502 U.S. at 400.

Moreover, courts have suggested that a consent decree's impact on local law enforcement activities is a factor to consider in assessing the continued viability of a consent decree. In *Alliance to End Repression v. City of Chicago*, the Seventh Circuit reversed a district court's act of enjoining the City of Chicago from implementing new guidelines for FBI investigations that were inconsistent with a 1981 consent decree regarding surveillance of First Amendment

activities. *All. to End Repression v. City of Chicago*, 742 F.2d 1007, 1020 (7th Cir. 1984). The Seventh Circuit explained how Chicago's consent decree impeded law enforcement and possibly affected public safety:

> We doubt that any neutral observer would think it appropriate that the FBI should be governed by other than a uniform national set of investigatory standards—that it should operate under one set of constraints everywhere but Chicago, and under another and tighter set in Chicago, so that this city can become a sanctuary for nascent terrorist organizations. To some extent the FBI is unavoidably under a tighter rein in Chicago than elsewhere, because of the consent decree, which applies only to Chicago. But there is no reason to magnify the disparity by looking for conflict between two sets of general language—the general principles of the decree and the general principles of the Smith Guidelines.
>
> *Id.* at 1018–19.

Ultimately, the Seventh Circuit modified the *Alliance* consent decree, based largely on the decree's impact on the ability of the Chicago Police Department to effectively protect the public. Judge Posner explained:

> All this the First Amendment permits (unless the motives of the police are improper or the methods forbidden by the Fourth Amendment or other provisions of federal or state law, *see Alliance to End Repression v. City of Chicago*, *supra*, 742 F.2d at 1014–15, and cases cited there), but the decree forbids. The decree impedes efforts by the police to cope with the problems of today because earlier generations of police coped improperly with the problems of yesterday. Because of what the Red Squad did many years ago, today's Chicago police are fated unless the decree is modified to labor indefinitely under severe handicaps that other American police are free from. First Amendment rights are secure. But under the decree as written and interpreted, the public safety is insecure and the prerogatives of local government scorned**.** To continue federal judicial micromanagement of local investigations of domestic and international terrorist activities in Chicago is to undermine the federal system and to trifle with the public safety. Every consideration favors modification; the City has made a compelling case for the modification that it seeks.

All. to End Repression v. City of Chicago, 237 F.3d 799, 802 (7th Cir. 2001) (emphasis added).

Here, like was the case in Chicago in the 1990s and early 2000s, the Consent Decree impedes the Memphis Police Department's ability to "cope with the problems of today" because earlier generations of police were found by this Court to have acted improperly with the

problems of the 1970s. Because of what a few bad actors did in 1976, today's police officers in Memphis are "fated unless the decree is modified to labor indefinitely under severe handicaps that other American police are free from." *See* 237 F.3d at 802.

Because the law regarding surveillance of First Amendment activity has been clarified since the entry of the Decree, and because the Decree is unworkable and a detriment to public safety, as explained *infra*, Section I of the Decree should be vacated or significantly modified in the interest of public safety.

C. ISSUES REQUIRING THE COURT'S IMMEDIATE REVIEW

Recently, the Monitor, acting as the special master for the Court, made several specific findings related to the intersection of the Consent Decree with MPD's current and proposed policies, practice, and procedures, which the City believes necessitate immediate modification of the Consent Decree in order to maintain the safety of the public. *See* July 2019 Quarterly Report of the Independent Monitor (ECF No. 218) ("July Quarterly Report"); August 12, 2019 Letter from Monitor to City ("August 12 Letter"), attached as **Exhibit A**; August 21, 2019 Letter from Monitor to City ("August 21 Letter"), attached as **Exhibit B**; August 26, 2019 Letter from Monitor to Mark Glover ("August 26 Letter"), attached as **Exhibit C;** August 29, 2019 Letter from Monitor to Mark Glover ("August 29 Letter"), attached as **Exhibit D.**

The specific issues that trigger the City's need for immediate modification or vacation of Section I of the Consent Decree to ensure that MPD is able to protect the public are (1) the City's need to receive and share intelligence with federal agencies; (2) the need to continue participation in the Joint Terrorism Task Force and to receive information from the Tennessee Fusion Center; (3) the need to continue participation in the Multi-Agency Gang Unit; (4) the need to continue participation in CrimeStoppers; and (5) the need to share information with the Shelby County Sherriff's Department which operates security within Shelby County Schools.

1. The need to receive and share intelligence with federal agencies for the purpose of public safety

On July 16, 2019, the City Attorney, Bruce McMullen, requested from the Monitor approval to coordinate with the FBI and the Secret Service in preparation for the 2019 PSP Symposium on Violent Crime, which was attended by executives from the DOJ, FBI, DEA, ATF, and United States Marshall Service. *See* August 21 Letter, at Exhibit B.

On August 21, 2019, the Monitor responded to Mr. McMullen's request explaining that request to coordinate with the FBI and Secret Service raised two issues that implicate the Consent Decree:

> First, to the extent that "coordinat[ing]" with the FBI or the Secret Service includes sharing personal information, the City may not coordinate with those agencies, or any others, in planning for the symposium. Section H of the *Kendrick* Consent Decree prohibits the City from "maintain[ing] personal information about any person unless it is collected in the course of a lawful investigation of criminal conduct." § H(1). It also prohibits the City from sharing "personal information . . . collected in the course of a lawful investigation of criminal conduct" unless the recipient is "another governmental law enforcement agency then engaged in a lawful investigation of criminal conduct." § H(2). I read this language to impose two applicable restrictions: (1) entirely against the sharing of personal information collected in any way other than via lawful criminal investigation (as such information may not be maintained in the first instance); and (2) against the sharing of personal information collected via lawful criminal investigation unless such sharing is with another governmental law enforcement agency and that agency already is engaged in a lawful criminal investigation.
>
> The second restriction is straightforward, but the first warrants elaboration. As an initial matter, § C(1) of the consent decree broadly prohibits the City from "engag[ing] in political intelligence." Section B(4) defines "political intelligence" to include both "the gathering [and] . . . dissemination of information . . . relating to any person's . . . exercise of First Amendment rights." Together, the two provisions prevent the City from sharing information relating to any person's exercise of First Amendment rights.
>
> …
>
> The ultimate consequence of these four sections, B(4), C(1), H(1), and H(2), is that the City may collect personal information—related or unrelated to the exercise of First Amendment rights—only in the course of a lawful criminal

> investigation, and may share that information only with a governmental law enforcement agency that already is involved in a criminal investigation.
>
> ***Second***, the City may not "benefit from the Intel" acquired by the FBI, the Secret Service, or any other law enforcement agencies unless the City first verifies that the information was not acquired in any way that the consent decree prohibits the City from using. Section I of the *Kendrick* Consent Decree forbids the City to "encourage, cooperate with, delegate, employ or contract with, or act at the behest of, any local, state, federal or private agency, or any person, to plan or conduct any . . . activity . . . prohibited by th[e] decree." I read this restriction to place the onus on the City to verify that any information it receives from governmental law enforcement agencies, non-law enforcement agencies, public and private entities, and individuals satisfies the same standards as information lawfully collected by the City itself.

Id. at pp. 1-3 (emphasis in the original).

The Monitor then found that the City may not receive intelligence collected from the FBI — or from any law enforcement agency — unless the City "first verified that the information was not acquired in any way that the consent decree prohibits." *Id.* at p. 3.[2] The Monitor also concluded that if "the City receives criminal intelligence from a governmental law enforcement agency for the purpose of conducting or supervising the MPD's own investigation of criminal conduct, then the City's receipt of that information also may be subject to the authorization and reporting requirements of § G of the consent decree." *Id.*

During the hearing on August 27, 2019, the Court addressed the specific issue of the City's coordination with the FBI and Secret Service in preparation for the PSP Symposium on Violent Crime *in camera*. Subsequently, the Monitor memorialized his understanding of that *in camera* conference in a letter to the City explaining that the Court authorized:

> … a limited, non-precedential departure from § I [of the Consent Decree] for purposes of providing security and public safety for the symposium. That departure allows the City to receive intelligence from the FBI, the Secret Service, and other law enforcement agencies without first verifying that such intelligence was acquired consistently with the consent decree's requirements. As your email

[2] The Monitor initially verbally expressed the view to the City on a conference call on June 14, 2019, that such receipt of information *did not* violate the Consent Decree. *See* Exhibit B, August 21 Letter, at p. 3.

> correctly recites, this departure does not allow the City or the MPD to (1) request that other law enforcement agencies "plan or conduct any investigation, activity or conduct prohibited by th[e] decree," § I; or (2) act on any information the City receives that, on its face, reflects that it was acquired in some way that the consent decree prohibits.
>
> I do not understand Judge McCalla to have authorized a departure from § H. In other words, in my view, the City and the MPD remain fully bound by § H as they prepare for and work with other law enforcement agencies before and during the symposium. They thus may share personal information with other law enforcement agencies, as opposed to receiving it from them, only as prescribed by § H.
>
> (Exhibit D, August 29 Letter, pp. 1-2,).

While the City is grateful for the Court's allowance of this limited, non-precedential departure from § I of the Consent Decree so that it was allowed to work with the Secret Service and FBI to provide security for the Deputy Attorney General and other high ranking governmental officials, the Monitor's interpretation of the Decree leaves the City with a serious and unworkable dilemma. How can the City receive and share information with federal agencies, and any other law enforcement agency, federal or otherwise, without violating the Consent Decree going forward?

The Monitor's interpretation of § I of the Consent Decree requires MPD to vet every piece of intelligence it receives from any source, including but not limited to the FBI, the DOJ, the Department of Homeland Security, and state law enforcement agencies. (Exhibit B, August 21, 2019 Letter, pp. 2-3). If MPD cannot determine if the intelligence gathered by the other law enforcement agency was gathered in a way that did not violate the Consent Decree, the very receipt of that information is a violation of the Decree. *See id.* at p. 3 ("If intelligence collected by governmental law enforcement agencies is not verified before the City receives it, then the City's receipt of that intelligence would violate the consent decree."). This interpretation places MPD in the precarious position of operating in a law enforcement "blind spot."

First, MPD cannot require that a federal agency, such as the FBI or DOJ, certify that the information it shares with MPD was obtained in a way that is not violative of the Consent Decree. As a threshold issue, requiring that a federal agency verify every piece of intelligence before it is disseminated to the MPD could have the effect of delaying the transmission of an urgent piece of intelligence that could stop, for example, a mass shooting.

Notwithstanding the impracticability of timely verifying that intelligence was obtained in way that did not violate the consent decree, federal agencies are not bound by the Consent Decree, only the U.S. Constitution. Unlike MPD, they are not restricted in the methods and sources they use to gather intelligence. It is impractical to suggest that an agency not bound by the Consent Decree should voluntarily abide by that decree's restrictions and prohibitions. MPD has no power or authority to require any federal or other entity to comply.

These restrictions on the open and contemporaneous sharing of information and intelligence with federal agencies will severely hamper the ability of federal law enforcement and MPD to prevent potential crimes in the Memphis area. For example, if the FBI used an undercover Facebook account to surveil a person who made inflammatory statements that might be reasonably be construed as veiled threats against a particular religious group, MPD would not be able to receive that intelligence from FBI unless MPD first certified that the information was not gathered in violation of the Consent Decree.[3] Under the Decree, MPD arguably would not even be able to hear that the FBI has determined that there is a possible threat or how urgent the situation is because MPD would first have to determine how the FBI obtained the information and then attempt to go through the certification process. If MPD learned that an undercover account was used to surveil someone expressing his First Amendment rights, under the Monitor's

[3] In this hypothetical, the posts, while inflammatory, did not rise to the level of an identifiable criminal threat.

interpretation, it would not be able to receive the intelligence at all and, therefore, act on the potential threat.

Moreover, if the intelligence received from the other law enforcement agency pertains to a criminal investigation that might interfere with the exercise of First Amendment rights or incidentally result in the collection of First Amendment-protected information, such an investigation must be approved by MPD's police director pursuant to § G of the Consent Decree. (Exhibit B, August 21 Letter, p. 3). Using the example from above, not only would MPD have to verify that the intelligence about the person making inflammatory comments about the religious group was obtained in a manner that does not violate the Consent Decree — which it could not reasonably do — it would also require that the MPD's Police Director authorize the FBI's investigation pursuant to § G of the Consent Decree. Obviously, it is impossible to require that MPD's Police Director approve investigations initiated and conducted by the FBI. MPD is not aware of any other law enforcement agency in the country that is limited in such a way. In short, the City cannot effectively provide public safety under such conditions.

Furthermore, MPD receives hundreds of thousands of dollars in federal grant money in exchange for its open and full cooperation with the federal government. This federal money is critical to the ability of MPD to reduce crime and protect the citizens of Memphis. For example, the City of Memphis received two law enforcement federal grants for 2018. The City was awarded $714,055 from the Bureau of Justice Assistance via the Local Law Enforcement Crime Gun Intelligence Center Integration Initiative Grant, which is described as follows:

> The Local Law Enforcement Crime Gun Intelligence Center Integration (CGIC) Initiative, administered by BJA in partnership with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), is a competitive grant program that provides funding to state and local government entities that are experiencing precipitous increases in gun crime to implement comprehensive and holistic models to reduce violent crime and the illegal use of firearms within their

> jurisdictions by enabling them to integrate with their local ATF CGIC. The purpose of this initiative is to encourage local jurisdictions to work with their ATF partners to utilize intelligence, technology, and community engagement to swiftly identify firearms used unlawfully and their sources, and effectively prosecute perpetrators engaged in violent crime. The CGIC Initiative is part of the Project Safe Neighborhoods (PSN) Suite of programs, which is focused on reducing violent crime. The PSN Suite comprises PSN, Strategies for Policing Innovation, Innovative Prosecution Solutions, CGIC Initiative, National Public Safety Partnerships, Technology Innovation for Public Safety, Encouraging Innovation: Field Initiated, Innovations in Community-Based Crime Reduction, and Community Based Violence Prevention Demonstration, and these initiatives will coordinate proactively with the PSN team in the respective district of the United States Attorneys Office (USAO) to enhance collaboration and strengthen the commitment to reducing violent crime. Applicants must demonstrate this coordination with their USAO district PSN team in their submission.
>
> The City of Memphis will use the BJA funds to enhance the analytical capabilities of the police department by hiring a contract analyst and eventually, a permanent senior crime analyst, as well as, purchasing technology to increase the capability to conduct investigations to identify, arrest, and prosecute violent gun crime offenders.

See FY 18 CGIC Program (emphasis added), attached as **Exhibit E.**

The City of Memphis also received $417,224 from the Bureau of Justice Assistance in the form of its Technology Innovation for Public Safety ("TIPS") Addressing Precipitous Increases in Crime:

> The FY 2018 Technology Innovation for Public Safety (TIPS) Addressing Precipitous Increases in Crime is part of the Project Safe Neighborhoods (PSN) Suite of programs, which is focused on reducing violent crime. The TIPS Program is designed to enable strategic information sharing across crime-fighting agencies with identified partnerships to address specific local or regional crime problems. Often these efforts will require a multidisciplinary response involving law enforcement, analysts and/or investigators, information technology staff, public safety and/or first responders, adjudications and/or courts, corrections, human services organizations, and other stakeholders.
>
> The City of Memphis will use the BJA funds to increase the License Plate Reader (LPR) technology by securing six mobile brief case LPR systems to investigate violent gang crimes in their jurisdiction. During investigations, officers will greatly benefit from LPR technology to quickly be able to both read and store license plates for their cases.

See FY 18 TIPS Memphis (emphasis added), attached as **Exhibit F.**

The federal government has formally recognized the importance of sharing of criminal intelligence through its implementation of 28 CFR Part 23, attached as **Exhibit G.** The regulation recognized that:

> certain criminal activities including but not limited to loan sharking, drug trafficking, trafficking in stolen property, gambling, extortion, smuggling, bribery, and corruption of public officials often involve some degree of regular coordination and permanent organization involving a large number of participants over a broad geographical area. The exposure of such ongoing networks of criminal activity can be aided by the pooling of information about such activities. However, because the collection and exchange of intelligence data necessary to support control of serious criminal activity may represent potential threats to the privacy of individuals to whom such data relates, policy guidelines for Federally funded projects are required.
>
> 28 C.F.R. § 23.2 (emphasis added).

Because the City is bound by the restrictions in the Consent Decree, and after receiving the Monitor's interpretation of the Consent Decree, the City is in the untenable position of being instructed that it is prohibited from freely and immediately sharing intelligence with federal law enforcement agencies as set forth in 28 CFR Part 23. This restriction puts the City's current and future federal law enforcement grants at risk.

In sum, it is impossible for the City to vet all intelligence a federal agency seeks to share before the City receives it. Moreover, because MPD cannot require that a federal agency obtain the MPD's Director of Police authorization of a criminal investigation that might incidentally result in the collection of First Amendment information, the Decree as interpreted by the Monitor, is unworkable. These circumstances, which could not have been foreseen in 1978, make compliance with Section I of the Consent Decree impossible while maintaining law enforcement standards now expected across the country and necessary to protect the public. It is, therefore, respectfully submitted that Section I be significantly modified or entirely vacated in the paramount interest of public safety.

2. The need to continue participation in the Joint Terrorism Task Force and to receive information from the Tennessee Fusion Center.

Similarly, Section I of the Consent Decree severely restricts or prohibits MPD's participation in the FBI's Joint Terrorism Task Force. The FBI's Joint Terrorism Task Forces ("JTTFs") are the nation's front line on terrorism: small groups of highly-trained, locally-based, passionately-committed investigators, analysts, linguists, SWAT experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies. A JTTF fights domestic and foreign terrorism by chasing down leads, gathering evidence, making arrests, providing security for special events, conducting training, and collecting and sharing intelligence.[4]

JTTFs have been instrumental in breaking up cells like the "Portland Seven," the "Lackawanna Six," and the Northern Virginia jihad. They have foiled attacks on the Fort Dix Army base in New Jersey, on the JFK International Airport in New York, and on various military and civilian targets in Los Angeles. They have traced sources of terrorist funding, responded to anthrax threats, halted the use of fake IDs, and quickly arrested suspicious characters with deadly weapons and explosives.[5]

The regional JTTFs coordinate their efforts largely through the interagency National Joint Terrorism Task Force, working out of FBI headquarters, which ensures that information and intelligence flows freely among the local JTTFs.[6]

The Memphis-based JTTF includes members from the FBI, MPD, Shelby County Sherriff's Department, the Department of Homeland Security, Immigration and Customs Enforcement, and the Transportation Security Administration. The JTTF enables a shared intelligence base across many agencies, and creates familiarity among investigators and

[4] https://www.fbi.gov/investigate/terrorism/joint-terrorism-task-forces
[5] https://www.fbi.gov/investigate/terrorism/joint-terrorism-task-forces
[6] https://www.fbi.gov/investigate/terrorism/joint-terrorism-task-forces

managers before a crisis. *See* Affidavit of Director Rallings ("Rallings Affidavit") at ¶ 11, attached as **Exhibit H.**

In view of Section I's restrictions on joint operations, as currently interpreted by the Monitor, the City will no longer be able to participate in the JTTF, putting not only local public safety at risk, but also jeopardizing the safety of the greater region and, potentially, the nation. If MPD is cut off from the JTTF, the ability of MPD to learn of potential threats and connections among local, regional, and national criminal activity will be severely limited.

In the same vein, Section I limits MPD's receipt of information from the Tennessee Fusion Center ("TFC"). The Tennessee Fusion Center (TFC) is a team effort of local, state and federal law enforcement, in cooperation with the citizens of the State of Tennessee, for the timely receipt, analysis and dissemination of terrorism information and criminal activity relating to Tennessee.[7]

Housed within TBI Headquarters in Nashville, the TFC was created in response to the intelligence failures of September 11, 2001. Fusion Centers have been developed across the country to provide an avenue of communication to enhance information sharing between federal, state, and local law enforcement agencies. The collaborative effort of the partnered agencies provide and share resources, expertise, and information with the goal of maximizing the ability to detect, prevent, apprehend and respond to criminal and terrorist activity. The TFC uses intelligence information with an 'all crimes' approach. It provides a central location for the collection and analysis of law enforcement related information and produces a continuous flow of that information to the law enforcement community. The TFC forecasts and identifies emerging crime trends and gives assistance to law enforcement in criminal investigations.[8]

[7] https://www.tn.gov/tbi/law-enforcement-resources/tennessee-fusion-center.html
[8] https://www.tn.gov/tbi/law-enforcement-resources/tennessee-fusion-center.html

The TFC consists of TBI employees as well as liaisons from the Tennessee Department of Safety & Homeland Security, Department of Correction, Board of Parole, the National Guard, ROCIC, ATF, and the FBI. TBI's Criminal Intelligence Unit ("CIU") houses the Fusion Center. CIU concentrates its effort on combating organized crime, gang activity, drug trafficking, Medicaid fraud, and fugitives. The CIU manages programs such as AMBER Alert, the statewide Sex Offender Registry, and the TBI Top Ten Most Wanted program. It is also the state's clearinghouse for missing and exploited children.[9]

As explained in detail above, it is not possible for MPD to vet every piece of intelligence it receives from the TFC to ensure it was obtained in a manner not violative of the Consent Decree. Even if it were possible, MPD would be expending precious resources and losing valuable time that would otherwise be focused on law enforcement, leading to more criminal activity and impairing MPD's ability to prevent and solve crimes. Moreover, it is also not practicable or feasible to require that the TFC obtain the Memphis Police Director's approval before initiating an investigation that might incidentally interfere with a person's First Amendment rights. Section I, as interpreted, thus prohibits MPD from receiving any information from the TFC going forward. This is an outcome, one can safely assume, that was neither intended nor desired by the drafters of the Consent Decree.

3. The need to continue participation in the Multi-Agency Gang Unit.

For many of the reasons set forth in Section II.C, *supra*, the City's participation in the Multi-Agency Gang Unit ("MGU") implicates and potentially violates Section I of the Consent Decree, as interpreted by the Monitor.

The MGU was formed in 2011, and is a group of elite highly-trained members of the Shelby County Sheriff's Office Narcotics Division, Memphis Police Department Organized

[9] https://www.tn.gov/tbi/law-enforcement-resources/tennessee-fusion-center.html

Crime Unit, ATF, FBI, and the U.S. Marshals. The MGU's mission is to conduct long term investigations on criminal gangs, to dismantle gang organizations, and to disrupt the illegal activities perpetrated by gang members. (Rallings Affidavit, ¶ 14.)

Since its inception, the MGU has been very successful. To take a recent example, in June 2019, a federal jury found five members of the Conservative Vice Lords Concrete Cartel criminal gang guilty of conspiracy to participate in racketeering activities, multiple armed pharmacy robberies, and drug trafficking conspiracy. One of the defendants was a Tennessee statewide gang leader and another was a citywide gang leader. The remaining defendants were branch leaders in the organization, claiming areas in East Memphis, Orange Mound, and Whitehaven. This federal prosecution and guilty verdict was the result of an extensive investigation which began in 2015 by FBI's Safe Streets Task Force and the MGU. (Rallings Affidavit, ¶¶ 15-16.)

Another example of MGU's success is the implementation of several "gang injunctions." In September 2013, as the direct result of MGU investigations into reports of criminal gang activity in the Riverside area of South Memphis, the Shelby County District Attorney's Office filed the first nuisance petition against the "Riverside Rollin' 90's Neighborhood Crips" ("R90"). In response to the petition, General Sessions Court Judge Larry Potter issued an injunction against R90 members, creating a 4.6-square-mile "safety zone." This process was followed three more times to obtain five more injunctions: (1) October 2014 against the "Dixie Homes Murda Gang/47 NHC" ("DHMG") in the North Main precinct; (2) December 2014 for two injunctions against the "FAM Mob" in two areas of the Old Allen precinct; and (3) January 2016 for injunctions against the "Grape Street Crips" (GSC) and "Vice Lords" (VL) in two overlapping areas of the Tillman Precinct. In each instance, the gang was declared a "public nuisance," and

members were required to abide by eleven requirements with respect to their behaviors in the safety zones. (Rallings Affidavit, ¶¶ 17-19.)

A preliminary assessment conducted by the University of Memphis's Public Safety Institute reveals that these gang injunctions are having a positive effect on the reduction of crime in the safe zones. Violent offenses in the zones have dropped nearly 8 percent from 2014 through 2018, and the number of violent offenses decreased in four of the six zones. *See* Public Safety Institute Interim Assessment of Gang Injunctions and Safety Zones in Memphis, attached as **Exhibit I.**

Participation in the MGU necessarily implicates § I of the Consent Decree, as currently interpreted, because the MGU requires open, free-flowing information among all the participating agencies. Because the Consent Decree, as interpreted by the Monitor, prohibits MPD's receipt of intelligence from another law enforcement agency unless vetted prior to its receipt to ensure it was obtained in a manner not violative of the Consent Decree, MPD effectively can no longer participate in the MGU. MPD is a critical member of the MGU, given its expertise and experience in gang-related law enforcement work. If MPD cannot participate in the MGU, public safety is gravely at risk. This risk can be mitigated through the modification or elimination of Section I of the Consent Decree.

4. The need to continue its participation in the CrimeStoppers program

The CrimeStoppers program is also implicated by Section I of the Consent Decree. CrimeStoppers is an independent, nonpartisan, nonprofit, citizen-run organization whose objective is to fight crime and bring criminals to justice.[10]

A telephone number maintained by CrimeStoppers receives anonymous tips regarding unsolved felony crimes and fugitives wanted. The anonymous tips are then forwarded to the

[10] http://crimestopmem.org/

appropriate law enforcement agency. The tipster is provided with a secret number that becomes the tipster's identity and means of staying anonymous. CrimeStoppers pays a reward to the tipster once a suspect is arrested and charged. Since 1981, CrimeStoppers "has helped solve thousands of crimes and stopped thousands of criminals."[11]

Because CrimeStoppers funnels intelligence related to criminal activity, *i.e.* anonymous tips, MPD's receipt of that intelligence is governed by Section I of the Consent Decree. The Monitor explained:

> Section I forbids the City to "encourage, cooperate with, delegate, employ or contract with, or act at the behest of, any local, state, federal or private agency, or any person, to plan or conduct any . . . activity . . . prohibited by th[e] decree." As stated in the August 21. 2019, Coordination Opinion, I read this restriction to place the onus on the City to verify that any information it receives from governmental law enforcement agencies, non-law enforcement agencies, public and private entities, and individuals satisfies the same standards as information lawfully collected by the City itself.
>
> Information collected by civilian residents of the City, shared with Crime Stoppers, and then shared with the MPD ordinarily would not implicate the First Amendment. The First Amendment restrains only the government, and not private individuals or organizations. Thus, the practices of private individuals and organizations do not offend the First Amendment even when those same practices, employed by the government, would violate it.
>
> Section I of the consent decree, however, forbids the City to coordinate both with governmental entities—"any local, state, [or] federal" entity—and with any "private agency, or any person, to plan or conduct any . . . activity . . . prohibited by th[e] decree." As a result, the practices of private individuals or organizations may offend the consent decree if the City "encourage[s], cooperate[s] with, delegate[s], employ[s] or contracts] with, or act[s] at the behest of' such private individuals or organizations "to plan or conduct any . . . activity . . . prohibited by th[e] decree." § I.
>
> The only way to ensure that the City does not offend the consent decree in working with private individuals or organizations is to require the same verification process for information received from private individuals and organizations as I understand the consent decree to impose for receiving information from the FBI, the Secret Service, or any other law enforcement agencies. (See generally August 21, 2019, Coordination Opinion.) The City's

[11] http://crimestopmem.org/

> ability to receive information from private citizens, either through Crime Stoppers or directly, is thus subject to verification that the information satisfies the same standards as information lawfully collected by the City itself.

(Exhibit C, August 26, 2019 Letter, pp. 10-11).

It would be literally impossible for the City to determine whether the information it receives from anonymous tipsters via CrimeStoppers was obtained in such way that does not violate the Consent Decree. The very element of the program that makes it successful is the preservation of the anonymity of the tipster. If the MPD tried to vet the tips that were provided, it would necessarily have to ascertain the identity of the tipster. This would effectively end the program, resulting in fewer prosecutions of crimes.

CrimeStoppers has been wildly successful in the Memphis and Shelby County region. In 2019 alone, tips received from CrimeStoppers has resulted in 216 felony arrests. These arrests have allowed law enforcement to resolve 135 cases this year, including 17 homicides.[12] If the Consent Decree prohibits MPD from participating in CrimeStoppers, crimes like those that were solved here will remain unsolved, and Memphis will be less safe, as a result. For that additional reason, Section I of the Consent Decree should be largely modified or set aside.

5. The need to receive and share personal information regarding juveniles with the Shelby County Sherriff's Department, which operates security within several Shelby County Schools.

Another "joint operation" implicated by Section I of the Consent Decree involves MPD's interaction with Shelby County Schools. First, the Shelby County Sheriff's Department provides security via its deputies within several local schools. Shelby County Sherriff's deputies often receive intelligence from students of potential gatherings that are planned that could end in a fight, or worse, a shooting. Under Section I of the Consent Decree, MPD is not permitted to receive that intelligence unless it first validates that the intelligence was gathered in a way that

[12] http://crimestopmem.org/

does not offend the Consent Decree. This would likely be impossible because the student tipster who provided the information to the deputy would be unlikely to provide his source for that intelligence for fear of reprisal. (Rallings Affidavit, ¶¶ 24-25.)

Indeed, Shelby County Schools recognized that students are often unwilling to publicly come forward with tips regarding past or potential crimes and implemented the Safe School Tips program. This service allows any parent, student, or employee to report information about illegal, potentially illegal, or inappropriate activities via text message anonymously anytime someone has a safety concern for herself or other students.[13]

Because the tips received from Safe School Tips are submitted anonymously, MPD has no way of determining if the intelligence contained in the tips was collected in a permissible manner under the Consent Decree. This inability to receive and act on anonymous tips from students leaves the student population of Shelby County much less safe.

Moreover, the City, Shelby County, and CrimeStoppers collaborate on a program called "Trust Pays." Trust Pays offers a safe way for students to confidentially inform a school administrator of a serious incident and potentially receive a cash reward as a result The Trust Pays program operates in elementary, middle and secondary schools. Trust Pays provides a safer learning environment for staff and students by reducing the incidents of weapons, drugs and violence on Shelby County Schools campuses.[14] For the same reasons as outlined in Section B.4. *supra*, Trust Pays will be severely impacted if MPD is required to adhere to the interpretation of Section I of the Consent Decree as put forth by the Monitor.

Indeed, the Consent Decree, as interpreted by the Monitor, precludes MPD from receiving information, from students or otherwise, gathered as part of the Department of

[13] http://www.scsk12.org/safe/
[14] http://www.scsk12.org//safety/programs?PID=649; http://www.crimestopmem.org/trust_pays.html;

Homeland Security's "If You See Something, Say Something" campaign. The "If You See Something, Say Something" campaign works with partners to educate the public on suspicious activity reporting. The campaign calls on citizens and the public to learn the indicators of terrorism-related suspicious activity and to notify local law enforcement of anything suspicious.[15] For the reasons explained *supra*, MPD can no longer receive this type information from a citizen because it would not be able to guarantee that the information was not obtained in violation of the Consent Decree.

The drafters of the Consent Decree could not possibly have foreseen the varied and significant restrictions Section I would impose on MPD forty years in the future. It is respectfully submitted that Section I should be set aside or significantly modified in the interest of public safety.

III. CONCLUSION

The City understands that, absent a modification such as the one requested here, the Monitor was required to interpret the Consent Decree as it is currently worded. For that reason, as well as the reasons set forth above, and subject to further proposed modifications or revisions as considered reasonable or necessary by the City, the City respectfully moves to vacate, or substantially modify, Section I of the Consent Decree. The City further respectfully requests that the Court permit it to continue its participation with the agencies listed *supra* while the Court considers this Motion in the interest of public safety.

[15] https://www.dhs.gov/see-something-say-something

Respectfully Submitted,

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

s/ Jennie Vee Silk

Buckner Wellford (#9687)
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: bwellford@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 September 25, 2019 the foregoing will be served by this Court's ECF system to:

Thomas H. Catelli, Esq.
Mandy Floyd, Esq.
Legal Director
ACLU Foundation of Tennessee
Post Office Box 120160
Nashville, Tennessee 37212

s/ Jennie Vee Silk

EXHIBIT A

BUTLER | SNOW

August 12, 2019

VIA ELECTRONIC AND U. S. MAIL

R. Mark Glover, Esq.
Baker Donelson
Bearman, Caldwell & Berkowitz, PC
2000 First Tennessee Building
165 Madison Ave.
Memphis, TN 38103

Re: *ACLU-TN v. City of Memphis*, Case No. 2:17-cv-02120-JPM-jay:
The Monitoring Team's Responses to the City's June 7, 2019 Inquiries

Dear Mark:

I hope that you're well. Please find enclosed with this letter the Monitoring Team's responses to the City's inquiries of June 7, 2019. In making these recommendations, the Monitoring Team has sought to remain faithful to the court's mandate that it "ensure [the City's] compliance with the [*Kendrick* Consent] Decree and . . . provide closer guidance on what constitutes political intelligence." (ECF No. 151, PageID # 6275.) To the extent that, in the City's view, the consent decree's requirements raise public-safety concerns or otherwise implicate issues beyond the scope of that mandate, those concerns and issues are best addressed to the court in the first instance.

Responses to discrete requests for authorization raised by the City since June 7, 2019, are forthcoming in separate correspondence.

I look forward to our weekly call this Friday.

Sincerely,

BUTLER SNOW LLP

Edward L. Stanton III

Post Office Box 171443
Memphis, TN 38187-1443

EDWARD L. STANTON III
901.680.7369
edward.stanton@butlersnow.com

Crescent Center
6075 Poplar Avenue, Suite 500
Memphis, TN 38119

T 901.680.7200 • F 901.680.7201 • www.butlersnow.com
BUTLER SNOW LLP

ES:tw

cc: Bruce A. McMullen, Esq. (via email only)
Jim Letten, Esq. (via email only)
Gadson W. Perry, Esq. (via email only)

BUTLER | SNOW

Confidential Attorney Work Product

M E M O R A N D U M

To: The Monitoring Team

From: Edward L. Stanton III

Date: August 12, 2019

Subject: City's Responses to Monitoring Team's Feedback

OVERVIEW

As you are aware, the Monitoring Team and the ACLU-TN have had the opportunity to review and give feedback on several of the City of Memphis's policies and procedures that are implicated by the *Kendrick* Consent Decree. (*See* ECF Nos. 197, 205.) In addition to offering this feedback, the Team has also responded to the City's request for recommendations regarding eleven hypothetical scenarios. (*See* ECF 197-3.)

On June 7, 2019, the City sent the Monitoring Team its latest responses to the team's feedback on its revised policies and procedures and the recommendations made in response to the City's hypothetical scenarios. Please provide your feedback regarding the same as you did with the prior submissions. The feedback will be reconciled and provided to the City.

I. The City's Proposed Policies and Training Materials

A. Departmental Regulation 138 Political Intelligence (Revised)

Team's Prior Feedback to City of Memphis	City of Memphis's Response to Team's Prior Feedback	City of Memphis's Proposed Action in Response to Team's Prior Feedback	The Team's Response to the City's Proposed Action.	Recommendation(s)
The Team recommended that the definition of First	***Response***: The City accepts the recommendation.	The City adds the recommended language.	***Response***: The Team agrees.	The Team does not recommend anything further.

Amendment rights expressly include the right to petition the government. (ECF 197-1, PageID 6853.)				
The Team recommended adding language to the fourth paragraph of the policy as follows: "No member **shall knowingly, intentionally or recklessly facilitate or cause the interception, recording, transcription of— or otherwise interfere with or cause, any interference with any communications** by means of electronic or covert surveillance for the purpose of gathering political intelligence." (ECF 197-2, PageID 6866)	***Response***: The City accepts the recommendation.	The City adds the recommended language.	***Response***: The Team agrees, but it recommends revising this section for clarity.	Team recommends that this statement be revised as follows: "No member **shall knowingly, intentionally, or recklessly facilitate or cause the interception, recording, transcription of— or otherwise interfere with or cause any interference with— any communications** by means of electronic or covert surveillance for the purpose of gathering political intelligence."
The Team recommended	***Response***: The City accepts the	The City adds the	***Response***: The Team	The Team does not recommend anything

revising the second sentence in the fourth paragraph as follows: "No member shall engage in any action or disseminate damaging, derogatory, false or anonymous information about any person which will deprive any individual of their First Amendment Rights; nor will any member encourage, cooperate with, or contract with any local, state, federal or private agency to plan or conduct any **investigation involving political intelligence or for the purpose, expectation or anticipation of political intelligence."** (ECF 205, PageID 7078.)	recommendation.	recommended language.	agrees.	further.
The Team recommended that Paragraph 3, which states that	***Response***: The City accepts the recommendation.	The City proposes a time limit of ten days for	***Response***: The Team mostly agrees, but it	The Team recommends that the City establish a time limit of five calendar

"any member conducting or supervising such an investigation must bring the matter to the attention of the Director of Police Services, or his/her designee, for review and written authorization," have a time limit for notification added – for instance, "…prior to initiating such an investigation, or, where the possibility of such incidental receipt is discovered after an investigation has commenced, no later than [X] days after such discovery." (ECF 197-1, PageID 6853.)		bringing such an investigation to the attention of the Director or his/her designee.	recommends shortening the time limit for bringing the investigation to the attention of the Director or his/her designee. ***Rationale***: The Team believes that ten days is too long to wait to notify the Director of Police Services or his/her designee.	days.
The Team recommended revising the fifth paragraph to include language that investigations into unlawful conduct "**that reasonably may be expected to result**"	***Response***: The City accepts the Team's revised recommendation.	The City revises paragraph five to track the original language of revised DR 138. "Investigations into unlawful conduct that	***Response***: The Team disagrees. ***Rationale***: After further consideration, the Team believes the objective "reasonable person"	Team recommends that the City adopt the "reasonably may be expected to result" language that it previously recommended.

incidentally in the receipt of political intelligence require approval, but then the Team revised its recommendation to track the original language in paragraph five. (ECF 205, PageID 7078).		may incidentally result in the receipt of information relating to the First Amendment rights are permissible but require approval by the Director of Police Services or his/her designee."	standard should be applied and explicitly stated.	
The Team recommended adding language to the fifth paragraph stating, "An extension may be granted in writing by the Director or his/her designee for periods of up to an additional ninety (90) days; **and in extraordinary circumstances where warranted, additional 90-day periods as documented and approved by the Director or his Designee**." In the First	***Response***: The City accepts the revised recommendation.	The City adds the recommended language.	***Response***: The Team agrees.	The Team does not recommend anything further.

Quarterly Report, however, the Team revised its recommendation as follows: "The Police Director or his / her designee may grant written extensions of the initial ninety (90)-day period of up to 90 days each when such extensions are justified by extraordinary circumstances. For each such extension, the following two conditions must be satisfied: (1) The Director or his / her designee must consult with the City Attorney or the City Attorney's designee (who must be a lawyer in good standing with the Tennessee Board of Professional Responsibility); and (2) The investigating officer must complete the [Kendrick				

Consent Form] and state in writing either the persistent facts that establish extraordinary circumstances or new facts that do the same." (ECF 205, PageID 7078.)				

B. Memphis Police Department Political Intelligence Training for the Office of Homeland Security, the Real time Crime Center, and the Command Staff

Team's Prior Feedback to City of Memphis	**City of Memphis's Response to Team's Prior Feedback**	**City of Memphis's Proposed Action in Response to Team's Prior Feedback**	**The Team's Response to the City's Proposed Action.**	**Recommendation(s)**
The Team recommended that the training plan incorporate the use of hypothetical examples. The Team also recommended that training options include the following: providing a one- to two-hour block taught by an instructor who prepares a lesson plan	***Response***: The City accepts the recommendation.	The City adds four bullet points to the end of the Training Plan to address the Team's recommendation: ·All training on the *Kendrick* Consent Decree and its prohibition against political intelligence shall incorporate the use of hypothetical examples of permissible and prohibited	***Response:*** The Team agrees, but it recommends further revising the plan to include training on First Amendment topics as well. ***Rationale:*** The Team believes that it is important for officers	The Team recommends revising the training plan as follows: ·All training on the **First Amendment and the** *Kendrick* Consent Decree and its prohibition against political intelligence shall incorporate the use of hypothetical examples of permissible and prohibited conduct under the **First Amendment and the** *Kendrick* Consent Decree.

and course evaluations; building the training into existing training models; and using short officer training videos, known as video alerts. (ECF 197-1, Page ID 6854.)		conduct under the Kendrick Consent Decree. ·Training on the *Kendrick* Consent Decree shall be provided in blocks anticipated to be one- to two-hours long. The training will be conducted by an instructor with a written lesson plan. After each training session, the participants of the session will submit a course evaluation to the instructor. ·Training on the *Kendrick* Consent Decree shall also be incorporated into existing training models, such as routine training of police cadets at the Training Academy. ·Training on the *Kendrick* Consent Decree shall also be conducted via short officer training videos known as video	to understand First Amendment rights in order to understand what it is and is not permissible under the *Kendrick* Consent Decree.	·Training on the **First Amendment and the** *Kendrick* Consent Decree shall be provided in blocks anticipated to be one-to two-hours long. The training will be conducted by an instructor with a written lesson plan. After each training session, the participants of the session will submit a course evaluation to the instructor. ·Training on the **First Amendment and the** *Kendrick* Consent Decree shall also be incorporated into existing training models, such as routine training of police cadets at the Training Academy. ·Training on the **First Amendment and the** *Kendrick* Consent Decree shall also be conducted via short officer training videos known as video alerts.

		alerts.		
The Team recommended adding a requirement that the training be updated annually to track changes in relevant laws and MPD policies. (ECF 197-2, PageID 6869.)	***Response***: The City accepts the recommendation.	The City adds a bullet point to the end of the Training Plan to address the Team's recommendation. ·Training on the *Kendrick* Consent Decree shall be updated annually to track changes in relevant laws and MPD policies.	***Response:*** The Team agrees, but it recommends further revising the plan to include training on First Amendment topics as well. ***Rationale:*** The Team believes that it is important for officers to understand First Amendment rights in order to understand what it is and is not permissible under the *Kendrick* Consent Decree.	The Team recommends revising the training plan as follows: ·Training on the **First Amendment and the** *Kendrick* Consent Decree shall be updated annually to track changes in relevant laws and MPD policies.
The Team recommended that training be provided to all officers and civilian	***Response***: The City partially accepts the recommendation. ***Rationale***: While	The City proposes that within 21 days after approval of the training materials by the	***Response***: The Team disagrees. ***Rationale***: The Team	The Team recommends that the following policy be adopted: "Within 21 days after

employees working within or otherwise assigned or detailed to the Memphis Police Department. (ECF 197-1, PageID 6854.)	such a training program could be accomplished by use of the regular annual in-service training for officers, the City believes that the immediate training of such additional persons is outside the scope of the Order (ECF 151) listing groups to be trained initially, and would not be possible in a short time frame, particularly the 21 day period suggested by the City in its original submission.	Court, the City will begin training sessions for all officers and civilian employees of OHS, RTCC, and Command Staff. MPD will then begin to train all other MPD officers on the prohibitions of the Consent Decree. Due to the large number of officers (2000+), this training will be done on a rolling basis, with all officers and civilian employees of MPD to complete the training within 12 months.	recognizes the potential logistical problems with the immediate training of all officers; however, it believes that such training is necessary to ensure that the entire police department complies with the *Kendrick* Consent Decree. The Team also believes that such training is necessary to ensure that the topics become fully engrained within the entire MPD.	approval of the training materials by the Court, the City will begin training sessions for officers and civilian employees of specialized units including, but not limited to, the Office of Homeland Security, RTCC, Command Staff, and units investigating narcotics, violent crimes, gangs, organized crime, and intelligence. **The City will make every effort to complete these training sessions as soon as possible, but in no event later than December 31, 2019**. **Within 30 days after approval of the training materials by the Court, the City will provide and make available to all other MPD officers and employees a monitor-approved video alert on the First Amendment and the Consent Decree.** **MPD will also train all other MPD**

				officers and employees on the First Amendment and Consent Decree. This training may be done on a rolling basis to be completed no later than December 31, 2020."

C. PowerPoint Presentation

Team's Prior Feedback to City of Memphis	**City of Memphis's Response to Team's Prior Feedback**	**City of Memphis's Proposed Action in Response to Team's Prior Feedback**	**The Team's Response to the City's Proposed Action.**	**Recommendation(s)**
The Team recommended adding language to the seventh slide "Harassment and Intimidation Prohibited," stating that a valid law enforcement purpose is required. (ECF 197-1, PageID 6855.)	***Response***: The City accepts the Team's recommendation.	The City adds the phrase "Absent a valid law enforcement purpose" to the third and fourth bullets on Slide 7.	***Response***: The Team agrees.	The Team does not recommend anything further.
The Team recommended "MPD shall not record...	***Response***: The City accepts the recommendation.	The City incorporates the reasonable effect	***Response***: The Team agrees.	The Team does not recommend anything further.

for the purpose of chilling the exercise of First Amendment rights or for the purpose of maintaining a record of that gathering, or where such recording will reasonably have the effect of deterring any person from exercising First Amendment rights." (ECF 197-2, Page ID 6870.)		language to Slide 7.		
The Team recommended updating Slide 4 with the revised DR 138. (ECF 197-2, PageID 6869-6870.)	***Response***: The City accepts the recommendation.	The City updates as recommended.	***Response***: The Team agrees.	The Team does not recommend anything further.
The Team recommended updating PowerPoint to include language about non-collator social media searches. (ECF 197-2,	***Response***: The City accepts the recommendation.	The City updates Slide 12, Bullet 1 to include language about non-collator social media searches. "An MPD officer searches a	***Response***: The Team agrees.	The Team does not recommend anything further.

PageID 6871.)		social media collator **or platform** for all instances..."		
The Team recommended revising the language of Slide 14 to provide: "An MPD officer wearing a body camera that has been activated pursuant to MPD policy does not have to cover the camera every time he or she passes..." (ECF 197-2, PageID 6871.)	***Response***: The City accepts the recommendation.	The City includes the language.	***Response***: The Team agrees.	The Team does not recommend anything further.
The Team recommended that the City's examples of community organizers not single out one or two named groups. (ECF 197-2, PageID 6872.)	***Response***: The City accepts the recommendation.	The City removes all references to any particular group in the PowerPoint. Specifically, the City changed all instances of "Black Lives Matter" to "activist group."	***Response***: The Team agrees.	The Team does not recommend anything further.
The Team recommended deleting the language on	***Response***: The City declines the recommendation.	None.	***Response***: The Team disagrees.	The Team recommends adding language to Slide 14 that states,

Slide 14 regarding "kill the police," because any search of that term could incidentally collect information related to First Amendment rights. (ECF 197-2, PageID 6871.)	***Rationale***: The City does not agree with the Monitor's recommendation, because the Court used the example "kill police" in its Opinion and Order. (ECF 151.) The Court stated that a police officer who queries a social media collator for the phrase "kill police," is not going out of her way to "gather" information related to First Amendment rights, even though her action is definitely investigative in nature.		***Rationale***: The Team believes the First Amendment analysis to be more nuanced than the City's current position. The Team submits that collecting protected speech and considering its content is permissible so long as it is being done for a valid law enforcement purpose, in a manner that does not unduly infringe upon the ability of the speaker to deliver his or her message. In addition, there must be a reasonable relation between the collection and retention of the protected speech and the purpose of the investigation.	"Any use of this information, including its retention and dissemination, is governed by the Consent Decree."

D. **Guidelines for Delegation of Authority of Director of Police Services to Authorize Investigations That May Interfere with the Exercise of First Amendment Rights under Section G of the Kendrick Consent Decree**

Team's Prior Feedback to City of Memphis	**City of Memphis's Response to Team's Prior Feedback**	**City of Memphis's Proposed Action in Response to Team's Prior Feedback**	**The Team's Response to the City's Proposed Action.**	**Recommendation(s)**
The Team recommended adding language to this policy that requires review of each selected designee be made by competent in-house counsel or authorized/assigned counsel (ECF 197-1, PageID 6857.)	***Response***: The City accepts the recommendation.	The City has designated Attorney Zayid Saleem as the appropriate in-house counsel for this role.	***Response***: The Team agrees.	The Team does not recommend anything further.
The Team expressed concern that the volume of these investigations would be too voluminous for the Director to oversee and suggested adding language that the Designee submit a report to the Director. (ECF 197-1, PageID 6857.)	***Response***: The City agrees with the recommenda-tion.	The City notes that the policy already provides for the designee's report.	***Response***: The Team agrees.	The Team does not recommend anything further.
The Team recommended	***Response:*** The City accepts	The City includes this	***Response***: The Team agrees.	The Team does not recommend anything

revising the last sentence of the policy to state as follows: "The Director shall have the authority to rescind authorization for any investigation that the Director deems **to violate the letter or intent of the department prohibition against the gathering of political intelligence, or in cases in which either the initial, authorized investigative goals or purposes no longer exist; or when political intelligence collection is no longer merely incidental**." (ECF 197-2, PageID 6873.)	the recommenda-tion.	language.		further.
The Team recommended changing the temporal reporting requirement to the last Friday of every month **that is a regular business day**. (ECF 197-2, PageID 6873.)	***Response***: The City declines the recommenda-tion. ***Rationale:*** The City requests that the monthly	None.	***Response***: The Team disagrees. ***Rationale***: The Team believes that the directive should be specific enough that it's	The Team recommends changing the temporal reporting requirement to the last day of the calendar month. If the last day of the month is a weekend or state or federal holiday, the report should be due by the end of the next business day.

	reporting requirement not fall on a day certain, but rather just "monthly" due to the varying work schedules of those involved.		complied with and that account-ability is possible.	

E. Authorization for Investigations Which May Incidentally Result in the Collection of Information Related to the Exercise of First Amendment Rights Under Section G

Team's Prior Feedback to City of Memphis	**City of Memphis's Response to Team's Prior Feedback**	**City of Memphis's Proposed Action in Response to Team's Prior Feedback**	**The Team's Response to the City's Proposed Action.**	**Recommendation(s)**
The Team recommended that the policy define "situational assessment." (ECF 197-1, PageID 6858.)	***Response***: The City accepts the recommendation.	This definition is included in footnote 2.	***Response***: The Team agrees.	The Team does not recommend anything further.
The Team recommended adding a discussion of whether situational assessment reports should be excluded from the authorization process. (ECF	***Response:*** The City accepts the recommendation.	The City seeks to clarify this by changing the term "Situational Assessment Report" to "After Action Review." Accordingly, Number 6 is suggested to be revised as	***Response***: The Team agrees.	The Team does not recommend anything further.

197-1, PageID 6858.)		follows: "After Action Review (AAR)" is defined as a report following an incident describing the incident and analyzing MPD's preparation for and response or reaction to the incident.		
The Team asked for clarification about what policy governs the dissemination of First Amendment information to law enforcement referenced in the "Dissemination" section on page 3. (ECF 197-2, PageID 6874.)	***Response***: The City adds language to clarify.	The City adds the following language to the "Dissemination" section: "If the information collected related to the exercise of First Amendment rights as a result of an authorized investigation identifies a threat or potential disruption to a private entity, that information may be shared with the private entity's security and/or other joint law enforcement agencies as reasonably necessary."	***Response***: The Team disagrees and recom-mends additional language. ***Rationale:*** The Team believes that the language, as written, is too broad.	It is the view of the Monitoring Team that the City may ***not*** share political intelligence with any private person or any non-law enforcement entity under any circumstances under the *Kendrick* Consent Decree. We read § H of the consent decree to prohibit the sharing of personal information collected via a lawful criminal investigation ***unless*** such sharing is with another law enforcement entity ***and*** that entity already is engaged in a lawful criminal investigation. Thus, we do not believe that § H permits the City to share any information in an After Action Review with any private person or any non-law enforcement

				entity.
The Team recommended adding the following note at the end of the "Exclusions" section: "There may be times when an investigation starts out in one of the excluded categories and evolves into something that does not implicate First Amendment rights. Accordingly, officers involved in an investigation should remain vigilant for any changes that would trigger the need for authorization." (ECF 197-2, PageID 6875.)	***Response***: The City accepts the recommendation.	The City adds the recommended language.	***Response***: The Team agrees.	The Team does not recommend anything further.
N/a	N/a	N/a	N/a	The Team recommends adding the language of DR138 that explains the granting of written extensions past the initial ninety (90)-day investigation period. Thus this policy would include the following:

				"The Police Director or his/her designee may grant extensions of the initial ninety (90)-day period of up to 90 days each when such extensions are justified by extraordinary circumstances. For each such extension, the following two conditions must be satisfied: (1.)The Director or his/her designee must consult with the City Attorney or the City Attorney's designee (who much be a lawyer in good standing with the Tennessee Board of Professional Responsibility); and (2.) The investigating officer must complete [the *Kendrick* Consent Form] and state in writing either the persistent facts that establish extraordinary circumstances or new facts that do the same."

F. Form: Authorization for Investigations That May Incidentally Result in Political Intelligence

Team's Prior Feedback to City of Memphis	City of Memphis's Response to Team's Prior	City of Memphis's Proposed Action in	The Team's Response to the City's Proposed	Recommendation(s)

	Feedback	Response to Team's Prior Feedback	Action.	
Some members of the Team expressed concern that the ACLU-TN's recommendation that the Authorization Form include a separate section for the Director/Designee to list the precautions and techniques to be employed during the investigation to certify that they are the least intrusive means available might involve law enforcement sensitive methods, some of which could be secret or necessarily confidential. (ECF 197-2, PageID 6876.). The Team revised this recommendati	***Response***: The City accepts the prior, unrevised recommendation and responds to the request for clarification. The City responds to the request for clarification about types of precautions and techniques to be listed. "An example of a confidential technique that might be used in an investigation is the use of an undercover social media account aimed at accessing the private social media	The City deletes the section for the Director/Designee to list precautions and techniques to be employed during the investigation.	***Response***: The Team also requested further information from the City regarding examples of precautionary techniques. ***Note***: The City, in an email dated July 19, 2019, responded to the Team's precautionary techniques inquiry with the following: · Instructing the officer(s) conducting the search, after consultation with Atty. Zayid Saleem, to immediately destroy any materials obtained that do not have value in	After conferring with the ACLU-TN, the Monitoring Team would revise the first listed precautionary technique as follows: Instructing the officer(s) conducting the search, after consultation with the city's legal counsel that such materials shall be preserved until the conclusion of any ongoing criminal investigation, after which they must be returned to the individuals from whom they were obtained in order to ensure that any exculpatory or Brady materials are not destroyed or lost. In no event shall such materials be used for any purpose other than for a legitimate criminal investigation, nor shall any such materials relating to exercise of First Amendment rights be maintained, disseminated, or used in any manner that is inconsistent with or in violation of the *Kendrick* Consent Decree, the Court's Opinion and

on with a request for clarification about the kinds of information that would be provided by the City as precautions and techniques. (ECF 205, PageID 7079.)	account of a criminal suspect. Another law-enforcement sensitive technique that might be used during an investigation is the use of a court-ordered wiretap to monitor the phone calls between known gang members."		the criminal investigation. · where the search uncovers information pertinent to the criminal investigation but implicating a citizen's First Amendment rights, limiting the dissemination of that information to MPD "personnel with a need to know", and that group of recipients would be approved by the Director or his designee. · Using only open source, publicly available information. Investigating a closed account or use of an undercover account	Order of October 26, 2018 (ECF 151), available online at www.memphispdmonitor.com, or this department's policies relating to usage of social media and protection of individuals' First Amendment rights. In addition, the authorization form – or an attachment – must include more than a blanket statement that the four factors have been met, to ensure compliance with the decree and to facilitate auditing and oversight. The record must contain sufficient information to demonstrate, both internally and to the monitoring team's auditor, that authorizations are being considered on a case-by-case basis, based on the specific facts and justifications in an individual case. This should be done in a manner that does not risk disclosing genuinely confidential or law enforcement-sensitive information to the general public. The city should make a recommendation as to what that process would be, keeping in mind the

			requires a compelling reason subject to additional prior approval by the Director or his designees. O nce the investigation is over, the undercover account must "unfriend" or "unfollow" the person being investigated.	public interest in a transparent and accountable police department.
N/a	N/a	N/a	N/a	The Team recommends adding the language of DR138 that explains the granting of written extensions past the initial ninety (90)-day investigation period. Thus, after the sentence stating that an investigation will not exceed more than ninety calendar days, this form would state the following: "The Police Director or his/her designee may grant extensions of the initial ninety (90)-day period of up to 90 days each when such extensions are justified

				by extraordinary circumstances. For each such extension, the following two conditions must be satisfied: (1) The Director or his/her designee must consult with the City Attorney or the City Attorney's designee (who much be a lawyer in good standing with the Tennessee Board of Professional Responsibility); and (2) The investigating officer must complete [the *Kendrick* Consent Form] and state in writing either the persistent facts that establish extraordinary circumstances or new facts that do the same."

G. Written Guidelines for the use of Manual Social Media Searches and of Social media Collators (aka Using Social Media for Investigations)

Team's Prior Feedback to City of Memphis	**City of Memphis's Response to Team's Prior Feedback**	**City of Memphis's Proposed Action in Response to Team's Prior Feedback**	**The Team's Response to the City's Proposed Action.**	**Recommendation (s)**
The Team agreed with the ACLU-TN that the Social Media Policy	***Response***: The City accepts the recommenda-tion.	The policy applies to all MPD officers.	***Response***: The Team agrees.	The Team does not recommend anything further.

should apply to all MPD officers. (ECF 197-1, PageID 6860.)				
The Team recommended adding the following language regarding when the Social Media Guidelines are applicable: "The officer's personal use of the social media platform and any searches conducted for personal reasons are nevertheless subject to this reporting requirement, when: ·The information searched, gathered, collected, stored or disseminated involves, includes, intersects or overlaps with, or otherwise relates to or	***Response***: The City accepts the recommenda-tion.	The City adds the recommend-ed language.	***Response***: The Team agrees.	The Team does not recommend anything further.

has direct or derivative use in any investigation, inquiry or matter involving official law enforcement or department interest; and ·The officer has knowledge of such investigation, inquiry, or matter, or should reasonably have such knowledge." (ECF 197-1, PageID 6860.)				
The Team recommended that the "Documentation and Retention" Section be revised for clarity. (ECF 197-1, PageID 6861.)	***Response***: The City accepts the recommendation.	The City revises the section as follows: "Information gathered from a social media site by MPD related to First Amendment activity shall not be retained, unless for a legitimate	***Response***: The Team agrees but recommends amending the language for clarification. The Team also requests clarification about whether MPD has a policy section that generally authorizes audits of an officer's files? ***Note***: The City, in an email dated July 19, 2019,	The Team recommends amending the language as follows: "Unannounced **internal** audits of an officer's social media searches, etc."

		law enforcement purpose, for more than thirty days. All social media searches by an MPD officer shall be retained until reported to the Command Staff, which shall occur approximately every 90 days. At the end of each 90-day period, each MPD officer who conducted a search on social media must submit a list of search terms used to search the particular social media platform related to the officer's duties and responsibilities as an officer of the	responded to the Team's policy inquiry by providing the responsive policies and stating as follows: Yes. There are case status meetings which are held weekly throughout MPD. Each investigator meets individually with a supervisor to discuss cases in their Inform RMS folder that have not been disposed of within fifteen (15) days, in addition to past-due State Arrest Reports. The investigator should be able to articulate what steps are being taken to dispose of the cases in question, and the status of all overdue State Arrest Reports. Additionally, a supervisor must approve all State Arrest Reports and sign a checklist. The completed State Arrest Report file	

		MPD. These reports shall be submitted to the officer's commander. Unannounced audits of an officer's social media searches are permissible at any time for any reason when authorized by a member of the Command staff."	will be scanned and added to the records management as an object. The approving supervisor will make a notation in the records management task tab the date each State Arrest Report is approved. Finally, there is a weekly TRAC review. TRAC is MPD's weekly commander's meeting. One precinct is selected per week during TRAC and the precinct Commander brings his detectives to the meeting. A Deputy Chief reviews all Blue Crush designated crimes to include each original report along with the assigned investigator's supplemental report. Each report and investigation are discussed. An average of 40-50 cases are reviewed at this time.	

The Team recommended defining "Special Events." (ECF 197-1, PageID 6862.)	***Response:*** The City accepts the recommendation.	The City defines "special events" as the following: "Events, both planned and unplanned, that involves groups of people gathering in public which require the presence and planning of the City and/or MPD officers."	***Response***: The Team disagrees and requests that the City provide additional policies related to unplanned immediate events and/or flash mobs. ***Rationale***: The City's Public Assemblies and Application process uses different terms (special events, spontaneous events, and alternative events) than the proposed definition. This policy should be consistent with the City's Ordinance. ***Note*:** The City, in an email dated July 19, 2019, responded to the Team's policy request with the following: "MPD does not have a written policy specific to unplanned immediate events or flash mobs. MPD responds in a manner tailored to	The Team recommends revising the definition of "Special Events" to be consistent with the City's Ordinance on public assemblies.

			the specific nature of the event. MPD conducts 'After Action Reviews' of such an event. An After-Action Review is a report following an incident describing the incident and analyzing MPD's preparation for and response to the incident."	
The Team recommended adding a disciplinary requirement in the event of an officer's failure to adhere to the Social Media Policy as well as an auditing procedure. (ECF 197-1, PageID 6863.)	***Response***: The City accepts recommendation.	The City revises as requested.	***Response***: The Team agrees.	The Team does not recommend anything further.
The Team recommended that the policy state that an undercover social media account may not impersonate an actual person known to the subject of an investigation.	***Response***: The City accepts the recommendation.	The City revises as requested.	***Response***: The Team agrees but revises its recommendation.	The Team recommends revising the sentence "Under no circumstances may an officer impersonate an actual person known to the subject of an investigation through the use of an undercover social media

(ECF 197-1, PageID 6863.)				account" to say, "Under no circumstances may an officer impersonate an actual person through the use of an undercover social media account."
The Team recommended that a section regarding Juveniles be added. (ECF 197-1, PageID 6863.)	***Response***: The City accepts the recommendation.	The City adds the following language: ONLINE MONITOR-ING OF JUVENILES ON SOCIAL MEDIA "Any and all restrictions regarding the monitoring of juveniles included in MPD's practices, policies, or procedures, are incorporated into this Social Media Policy."	***Response***: The Team agrees but asks that the City share MPD's policies relating to juveniles so the Team can see how they would apply in the social media monitoring context. ***Note***: The City, in an email dated July 19, 2019, responded to the Team's request for juvenile policies by attaching the responsive policies.	The Team recommends adding the following language. "MPD officers are prohibited from using a social media account, including a covert account, to contact or connect with a minor without first notifying that minor's parent or guardian prior to initial contact. This policy may include exceptions for exigent circumstances and circumstances in which a parent or guardian is a subject of a predicated investigation."
The Team recommended clarifying a "situational assessment	***Response:*** The City accepts the recommendation.	The City revises the policy as follows:	***Response***: The Team mostly agrees but recommends that the City adds	The Team submits that any MPD investigation that uses social media as an investigative

report" vs. a "situational awareness report." (ECF 197-2, PageID 6879.)		"Situational awareness reports may be prepared for special events management, including First Amendment-protected activities. At the conclusion of the situation or First Amendment-protected event that was the catalyst for generation of a situational awareness report, and where there was no criminal activity related to the information gathered, the information obtained from social media or from a social media monitoring tool will be retained for no more than thirty (30)	language to the situational awareness report policy.	technique must have a lawful purpose and must not unlawfully infringe the First Amendment Rights of the individual(s) or groups subject to the investigation—meaning, the social media investigation should employ the least intrusive means upon exercise of those First Amendment rights. Further, if the investigation infringes on First Amendment rights, a rational connection between the collection of information about the individual(s) or groups and the purpose of the investigation should be documented. In addition, the Team further recommends the changes listed below.

		days. After Action Reviews may be prepared using information gathered from social media. "After Action Review" (AAR) is defined as a report following an incident describing the incident and analyzing MPD's preparation for and response or reaction to the incident. These reviews are aimed at department self-improvement. The information obtained from social media may be retained within the AAR indefinitely, but the		

		names, photos, and identifying information of individuals not suspected of criminal activity must be redacted." The City added in a footnote: "situational awareness report is report of intelligence gathered by law enforcement related to public safety surrounding a planned gathering of people in public. The purpose of a situational awareness report is to provide MPD with information so that it can adequately prepare for and protect the public before, during, and		

		after a special event."		
The Team recommended a shorter retention period for information about First Amendment activities. (ECF 197-2, PageID 6879.)	***Response***: The City accepts the recommendation.	The City includes the following language: "Information gathered from a social media site by MPD related to First Amendment activity shall not be retained, unless for a legitimate law enforcement purpose, for more than thirty days."	***Response***: The Team agrees.	The Team further recommends the changes listed below.
The Team requested clarification as to why the City made the change from allowing First Amendment information gathered on social media to be distributed only to the Command Staff versus "to MPD	***Response***: The City responds to request for clarification. The City made this change based on the ACLU-TN's suggestion. Moreover, the City envisions a situation in which some officer below the level of Command Staff	None.	***Response***: The Team is satisfied with the explanation.	The Team does not recommend anything further.

officers and staff as necessary." (ECF 197-2, PageID 6880.)	would be required to take an action (such as make an arrest) where access to the information would be critical.			
The Team recommended that there be audits of an officer's social media searches. (ECF 197-1, PageID 6863.)	***Response:*** The City accepts the recommenda-tion.	The City adds the following language to its policy: "Unan-nounced audits of an officer's social media searches are permissible at any time for any reason when authorized by a member of the Command Staff."	***Response***: The Team agrees but recommends amending the language for clarity.	The Team recommends amending the language of the policy as follows: "Unannounced **internal** audits…"
N/a	N/A	N/a	N/a	The Team recommends revising the title of the social media policy, which is currently "Utilizing Social Media for Investigations," to "Law Enforcement Utilization of Social Media," because the policy covers more than

				investigations.
N/a	N/a	N/a	N/a	The Team recommends changing all instances of "MPD officers" to "MPD employees" in the social media policy.
N/a	N/a	N/a	N/a	The Team recommends revising the sentence, "All searches of social media by a MPD officer, through the use of a social media account or social media collator…" to "**All searches of social media by an MPD employee, including but not limited to those through the use of a social media collator, shall be based on a valid law enforcement purpose**…."
N/a	N/a	N/a	N/a	The Team recommends adding the following language after the first paragraph under "Use of Social Media" on page three, or before the paragraph beginning "Social Media searches are

				limited to sources within the public domain..." on page four: "Social media may not be used to seek or retain information about: •An individual's race, ethnicity, citizenship, place of origin, disability, gender, or sexual orientation, unless relevant to individual's criminal conduct or activity or if required for identification; or •An individual's age, other than to determine if person is a minor."
N/a	N/a	N/a	N/a	On top page four of the social media policy, after the term "shoot the police," the Team recommends adding a sentence stating, "However, the use, retention, or dissemination of information collected by searches that relate to the exercise of First Amendment rights is governed by the

				Consent Decree."
N/a	N/a	N/a	N/a	On page four of the social media policy, the current policy says, "Only searches of open-sources (non-private) should be used." The Team recommends revising this to say, "Only searches of open source (non-private) information should be used."
N/a	N/a	N/a	N/a	On page five of the social media policy, the current policy states, "Information gathered from a social media site by MPD related to First Amendment activity shall not be retained, unless for a legitimate law enforcement purpose, for thirty days." The Team recommends shortening this to fourteen days. The Team also recommends revising the language under situational awareness reports, as stated on page six of the policy, to

				reflect this fourteen day retention requirement.
N/a	N/a	N/a	N/a	The Team recommends revising the last two paragraphs on page five of the social media policy to clarify the distinction between keeping information for a limited period (currently 30 days) and keeping the searches themselves for up to 90 days. The Team recommends adding language such as, "The terms used by an MPD officer to conduct social media searches shall be retained…"
N/a	N/a	N/a	N/a	The Team recommends revising the situational awareness reports language as follows: "Situational awareness reports may be prepared for special events management, including First Amendment-

				protected activities, where necessary for the furtherance of public safety. Employees preparing such reports must take special care to collect no more information than necessary regarding the exercise of First Amendment-protected rights. Employees should further document that there is a relationship between the incidental collection of information about First Amendment-protected activities and the purpose of the report, which is the protection of public safety. At the conclusion of the situation or First Amendment-protected event, the information obtained from social media or from a social media monitoring tool will be retained for no more than fourteen days."

N/a	N/a	N/a	N/a	With respect to After Action Reviews, the Team recommends adding "organization" to the final sentence – so it would say "…the names, photos, and identifying information of individuals **and organizations** not suspected of criminal activity should be redacted."

H. Social Media Search Terms

Team's Prior Feedback to City of Memphis	**City of Memphis's Response to Team's Prior Feedback**	**City of Memphis's Proposed Action in Response to Team's Prior Feedback**	**The Team's Response to the City's Proposed Action.**	**Recommendation(s)**
The Team expressed concerns about the certification process for social media searches by MPD officers. In particular the Team recommended that the MPD certify that each term has a	***Response***: The City requests follow-up information. The City would like clarification as to whether the Team is suggesting a certification be made for each	The City suggests that it maintain the current practice of reporting social media search terms from the limited set of phones as outlined in its pleadings to the Court (OHS, RTCC,	***Response***: The Team disagrees and requests more information about how many officers outside the officers covered by the policy also use social media for work. ***Note***: The City,	The Team recommends that the City create an internal audit system to ensure compliance by all MPD offices and civilians.

valid law enforcement purpose. (ECF 197-1, PageID 6864.)	individual search term as it is occurring in real time, or if a "blanket group certification" be made by each officer when he/she submits his/her search terms quarterly. To this point, the City notes that certifying each search term in real time would be incredibly onerous. The City is also doubtful whether the Court intended that every MPD officer's phone be subject to the social media search term reporting requirement.	General Investigative Unit, Homicide, Sex Crimes, and Command Staff). It also expresses concern that to require all 2000+ officers to submit search terms quarterly would be onerous.	in an email dated July 19, 2019, responded to the Team's request for social media use information with the following: "While no officer is directed or required to do so, we think it is reasonable to assume that every officer in the units listed above as well as every uniformed police officer within MPD may use social media for the purpose of a criminal investigation, consistent with the purpose and manner as the search terms used on social media that the City has been reporting since January 2019."	

The Team requested an explanation for the use of the word "protest" as a search term in conjunction with the words "St. Jude" and "marathon." (ECF 197-1, PageID 6864.)	***Response***: The City responds to request for information. The City states that those terms were used by Sergeant Eddie Cornwell from the Office of Homeland Security. The searches in question were performed around the time of the marathon to identify anyone who might be preparing to engage in acts threatening the safety of the event.	None.	***Response***: The Team is satisfied with the explanation.	The Team does not recommend anything further.

(2.) The Eleven Scenarios

Body Worn Cameras

City's Current Policy: MPD POP Chapter XIII, Section 15: In-Car Video/Body Worn Cameras. The relevant language is as follows:

> "Officers shall record all law-enforcement encounters and activities." (Page 3, ¶ B.3.).

"Once a recording event begins, the BWC shall remain activated until the event has concluded in order to conserve the integrity of the recording." (Page 4, ¶ B.6).

"Officers are responsible for the labeling and the categorization of videos they produce. The videos will be categorized in accordance with the available choices in the system. Officers will obtain the Computer Aided Dispatch number either through an automated feature, from the dispatcher, or through a manual lookup and entered in the ID field. (41.3.8G)

Officers who categorize videos incorrectly may be subject to discipline." (Page 5, ¶ B.9.)

"As a general rule, recordings classified as non-evidentiary will be retained for ninety days before deletion. Recordings classified as evidentiary will be retained for one year after any final legal disposition. Further, evidentiary data shall be retained for the period specified by any applicable state or local statute. When a particular recording is subject to multiple retention periods, it shall be maintained for the longest applicable retention period. (41.3.8G)" (Page 12, § IX.)

Scenario No. 1: When police officers are at the scene of a protest (either permitted or unpermitted) for purposes of public safety, may they leave their body cameras on even though First Amendment Rights are being exercised? ("First Amendment Rights" in this context means expressive conduct in the public sphere.) No film of protesters would be retained unless the film reflects a criminal act or provides important evidence with regard to a criminal act.

Team's Prior Feedback to City of Memphis	City of Memphis's Response to Team's Prior Feedback	City of Memphis's Proposed Action in Response to Team's Prior Feedback	The Team's Response to the City's Proposed Action.	Recommendation(s)

The Team requested clarification about whether the City is proposing that it be able to continuously record First Amendment activities, or that it be able to film discrete incidents that occur during the course of First Amendment activities. (ECF 197-3, PageID 6925.)	***Response***: The City proposes that it be able to continuously record First Amendment activities. ***Rationale***: The City believes that best practices would dictate that body cameras be activated at all times during a demonstration, protest, or other expression of First Amendment activity involving a group of people to ensure that all citizen interactions are recorded. This is necessary in the event that a disruption occurs that causes damage to property or the public. Moreover, if there was any question as to police misconduct, unequal or harsh treatment of one group over	The City, after further review, believes there is no policy it could enact that would allow the video recording of people exercising their First Amendment rights without the possibility of having a chilling effect on those people, and thus running afoul of the Consent Decree. The City intends to take it to the Court for further guidance.	***Response***: The Monitoring Team welcomes the input of the Court but makes the adjacent recommendation in the interim.	After conferring with the ACLU-TN, the Monitoring Team recommends the following: Body-worn cameras (BWCs) should not be rolling constantly at a First Amendment-protected special event or when a person is engaged in First Amendment protected activity in a public area, in the absence of a legitimate law-enforcement encounter. BWCs should only be activated for legitimate law-enforcement encounters, such as observing any ongoing criminal activity, including unlawful interference with another person's exercise of her or his First Amendment rights. Such rights include speaking or leafleting in a public area or at a special event permitted by the City. It is critical that MPD's BWC policy be enforced in an even-handed manner and

	another, or the use of unreasonable force, the body warn camera footage from the event would likely answer those questions.			that all MPD officers be thoroughly trained on what constitutes a legitimate law-enforcement encounter understanding every specific encounter requires the exercise of sound discretion and judgment on the part of the officer.
The Team acknowledged the benefit of ensuring that citizen interactions are recorded and the potential chilling effect that body worn cameras can have on those engaging in First Amendment activities. For that reason, the Team coalesced around two major views: (a) body cameras should activated at all times during a demonstration to ensure that all citizen	***Response:*** The City agrees with the First Amendment rights concerns and requests a final recommendation from the Team. ***Rationale:*** The Consent Decree expressly forbids the City of Memphis from engaging "in any action for the purpose of, or reasonably having the effect of, deterring any person from exercising First Amendment rights. As an example, the City of Memphis	The City intends to take issue to the Court for further guidance.	***Response:*** See response above.	See response above. In addition, the Team intends to hold a focus group directed at this issue.

interactions are recorded, and (b) body cameras should be activated only when an officer begins a voluntary or involuntary citizen interaction. (ECF 197-3, PageID 6925.)	shall not, at any lawful meeting or demonstration, for the purpose of chilling the exercise of First Amendment rights or for the purpose of maintaining a record, record the name of or photograph any person in attendance, or record the automobile license plate numbers of any person in attendance." (Consent Decree, § F.2., ECF No. 151, PageIDs 6282-83). Thus, the City agrees that the use of Body Worn cameras at a protest or demonstration likely offends the Consent Decree.			
The Team recommended creating a comprehensive policy manual that modifies and defines	***Response:*** The City did not address this.	None.	***Response:*** None	The Team stands by its prior recommendation.

certain terms used by the City in this policy and scenario. For example, the term "law-enforcement encounters and activities" is too broad. The City should specify the types of criminal investigations for which this would be authorized. As written, this policy potentially covers anything that an on-duty officer does in the course and scope of her duties, including walking or patrolling a beat. (ECF 197-3, PageID 6926.)				

Covert Social Media Accounts

City's Current Policy: *See* MPD Real Time Crime Center Standard Operating Procedure (SOP) .

> "Social Media
>
> ALL RTCC STAFF WILL FAMILIARIZE THEMSELVES WITH THE KENDRICK V. CHANDLER, CONSENT DECREE NO. C 76-449.
>
> Pursuant to the 1978 Kendrick Consent Decree, the Memphis Police Department will cease utilizing investigative and covert accounts on all social media platforms. The only account that may be utilized is that which is approved by The City of Memphis Legal team and the Court ordered monitor. The RTCC will not engage in the use of Social Media for any reason unless otherwise directed by the Command Staff." (§ 1.9.)

City's Proposed Covert Social Media Account Policy:

> The MPD shall not use investigative and covert accounts on any social media platform for the purpose of political intelligence. "Political intelligence" was defined in the 1978 Kendrick Consent Decree as "the gathering, indexing, filing, storage or dissemination of information, or any other investigative activity, relating to any person's beliefs, opinions, associations or other exercise of First Amendment rights." The provisions of the Kendrick Consent Decree prohibit MPD from "engaging in law enforcement activities which interfere with any person's rights protected by the First Amendment, including but not limited to, the rights to communicate an idea or belief, to speak freely, to write and to publish, and to associate privately and publicly for any lawful purpose."
>
> An MPD officer may use an alias to develop online relationships with individuals and gain access to private online groups as part of a criminal investigation. If a criminal investigation results in the collection of information about the exercise of First Amendment rights, or interferes in any way with the exercise of First Amendment rights, the criminal investigation must be reviewed and authorized by the Memphis Director of Police or his/her designee.

Scenario 2: May police officers work under cover by using social media accounts to discover, pursue and prosecute, or prevent possible crimes such as human trafficking, internet crimes against minors, child pornography, illegal drug sales, and related behavior even though entry into the social media platforms under cover may expose them to persons expressing views protected by the First Amendment?

Scenario 5: May police officers use "dummy" or "undercover" social media accounts to investigate crimes unrelated to First Amendment activity without Director approval pursuant to § G (e.g. using a "fake" Facebook account to investigate a suspected drug trafficking enterprise)?

Team's Prior Feedback to City of Memphis	**City of Memphis's Response to Team's Prior Feedback**	**City of Memphis's Proposed Action in Response to Team's Prior Feedback**	**The Team's Response to the City's Proposed Action.**	**Recommenda-tion(s)**
Regarding the proposed policy, the Team advised that the term "criminal investigations" is too broad and recommended that the language be modified to specify the types of crimes covered by this policy. (ECF 197-3, PageID 6927.)	***Response*:** The City accepts the Team's recommendation.	The City proposes defining "criminal investigation" in the amended policy as it is defined in the Social Media Policy as follows: "If probable cause exists that a crime has been committed, a criminal investigation is the process of collecting information or evidence about an incident in order to: (1) determine if a crime has	***Response:*** The Team disagrees and recommends amending the language of the proposed policy. ***Rationale***: The Team would like to emphasize the importance that such investigations should be for purposes other than to interfere with or gather information related to First Amendment activities.	The Team recommends that the proposed policy be amended as follows: "An MPD officer may use an alias to develop online relationships with individuals and gain access to private online groups as part of a criminal investigation; an alias may not be used **to interfere with or gather information related to First Amendment activities.** Moreover, even in circumstances where the purpose of the online alias is to

		been committed; (2) identify a perpetrator; (3) establish probable cause; (4) apprehend the perpetrator; and (5) provide evidence to support a conviction in court."		collect information related to a criminal investigation, the use of social media to connect with or monitor an individual will implicate First Amendment-protected rights. See Kendrick Consent Decree at p. 3, Para. G (Prohibition Against Covert Surveillance for Political Intelligence). "A police officer may, for example, need to "friend" a suspected drug dealer as part of an investigation. The officer in question would not be conducting political intelligence, because while he may incidentally obtain information relating to the suspect's exercise of First Amendment rights, he is not "gathering" that information. This officer does,

				however, need to seek formal approval through use of the authorization form, because the investigation "may result in the collection of information about the exercise of First Amendment rights." (Consent Decree, at § G.)'" Opinion And Order at p. 34 n.14 (Oct. 26, 2018) (ECF 151, PageID 6274 n.14.)
The Team advised that the proposed Covert Social Media Account Policy suggests that the use of undercover social media accounts for criminal investigations *per se* does not interfere with a person's First Amendment rights. The Team further advised that such a stance is inaccurate. The Team	***Response*:** The City accepts the advice and recommendation.	The City proposes adding the following language: "The use of undercover social media accounts may incidentally interfere with a person's First Amendment rights. In those cases, care must be taken to comply with the Kendrick Consent Decree and	***Response:*** The Team agrees but recommends that the policy also clarify the "care must be taken" language with a citation to the Consent Decree.	The Team recommends that the City cite and quote the provisions of the Consent Decree that address what the First Amendment and the Consent Decree prohibit, that is Consent Decree at B.4, C.1, and D-F."

recommended revising the policy. (ECF 197-3, PageID 6927.)		DR 138."		
The Team recommended that there be an auditing system to assess whether MPD is actually capturing, reviewing, and getting authorizations for undercover social media criminal investigations that result in the collection of First Amendment information. (ECF 197-3, PageID 6927-6928.)	***Response*:** The City accepts the Team's recommendation.	The City agrees and is working on ideas for such an auditing system which would employ random sampling and periodic full review.	***Response:*** The Team agrees.	The Team does not recommend anything further.
In terms of using social media accounts for specific investigation of crimes, the Team recommended: a. some predication required to open a matter and follow lead/institute active use; and	***Response***: The City requests clarification as to point (a) and accepted recommendation in point (b).	The City will make changes recommended in "b."	***Response***: A "Predication" is a term used often in federal enforcement. It means reason, purpose, or objective trigger for an investigation—as opposed to an unlawful or purely subjective reason for	The Team recommends the following language to supplant point "a": "A lawful purpose must be required to open a matter and institute a social media investigation."

b. in investigations in which no criminal conduct is intercepted, there be no retention of intercepted communications when using social media accounts for specific investigations of crimes. (ECF 197-3, PageID 6928.)			opening an investigation. With this in mind, the Team now borrows the term "lawful purpose" from FBI protocols and applies it here to supplant the term "predication." ***Rationale***: This change is meant to underscore the fact that such investigatory procedures must have articulable and lawful reasons for launching them.	
The Team clarified that it is not in the position to approve or disapprove of the City's "the investigative and covert [social media] accounts" that are covered by the January 10, 2019, policy. (ECF 197-3, PageID 6928.)	***Response***: The City understands the Team's stance.	The City is not seeking the Monitor's approval of any specific account, but of its policy generally.	***Response*****:** The Team is satisfied with this explanation.	The Team does not recommend anything further.

Scenario 3: May police officers work under cover by using social media accounts to investigate acts of domestic terrorism such as school bomb threats or school shooting threats which are reported to or discovered by them even though entry into social media platforms under cover may expose them to persons expressing views protected by the First Amendment?

Team's Prior Feedback to City of Memphis	**City of Memphis's Response to Team's Prior Feedback**	**City of Memphis's Proposed Action in Response to Team's Prior Feedback**	**The Team's Response to the City's Proposed Action.**	**Recommendation(s)**
The Team advised that the City's proposed Covert Social Media Account Policy would not adequately address any concerns about the implications of the Consent Decree. (ECF 197-3, PageID 6929.)	***Response***: The City accepts the Team's advice.	The City proposes adding the following language: "The use of undercover social media accounts may incidentally interfere with a person's First Amendment rights. In those cases, care must be taken to comply with the Kendrick Consent Decree and DR 138."	***Response*:** The Team agrees but recommends amending the policy to incorporate First Amendment compliance and clarifying the "care must be taken" language with a citation to the Consent Decree.	The Team recommends amending the policy as follows: "The use of undercover social media accounts may incidentally interfere with a person's First Amendment rights. In those cases, care must be taken to comply with the **First Amendment**, *Kendrick* Consent Decree, and DR 138." Further, the Team recommends that the City cite and quote the provisions of the Consent Decree that address what the First Amendment and the Consent Decree prohibit, that is Consent Decree at B.4, C.1, and D-F."
The Team advised that an investigative response to information	***Response***: The City agrees with the advice.	None.	***Response*:** The Team agrees.	The Team does not recommend anything further.

regarding ongoing or imminent violent acts is not only permissible but appropriate and necessary. (ECF 197-3, PageID 6929.)				

Scenario 6: May the MPD use all investigative techniques available, including the use of undercover and "dummy" social media accounts for the purpose of criminal intelligence development (defined as information relevant to the identification of criminal activity engaged in by individuals or organizations which are reasonably suspected of involvement in criminal activity) without Director approval pursuant to § G (e.g. the ongoing gathering of intelligence into a drug trafficking ring)?

Team's Prior Feedback to City of Memphis	**City of Memphis's Response to Team's Prior Feedback**	**City of Memphis's Proposed Action in Response to Team's Prior Feedback**	**The Team's Response to the City's Proposed Action.**	**Recommendation(s)**
The Team advised that to the extent that such investigations are targeting clearly illegal conduct (e.g., drug trafficking), the mere possibility that some protected conversations may be intercepted should not	***Response*: The** City declines the advice. ***Rationale***: The City believes its amended proposed Covert Social Media Account Policy is consistent with the Court's finding that the use of undercover accounts is	Maintain amended proposed Covert Social Media Account Policy.	***Response***: The Team disagrees. ***Rationale:*** Team believes that director approval is required here, because there is a possibility of collecting	The Team recommends revising this policy to be consistent with the Court's Order and Opinion, which states: "A police officer may, for example, need to 'friend' a suspected drug dealer as part of an investigation. The officer in question would not be conducting political intelligence, because

require additional approval. In the event protected communications are intercepted, policies should require immediate notification, reporting, approval, and handling that will prevent political use and dissemination. (ECF 197-3, PageID 6932.)	permissible under the Consent Decree.		First Amendment protected information.	while he may incidentally obtain information relating to the suspect's exercise of First Amendment rights, he is not 'gathering' that information. This officer does, however, need to seek formal approval through use of the authorization form, because the investigation 'may result in the collection of information about the exercise of First Amendment rights.' (Consent Decree § G.)" (ECF 151, PageID 6274 n.14.)
The Team disagreed with City's proposal that it adopt the federal guidelines on criminal intelligence found in 28 CFR Part 23 as its policy on criminal intelligence. (ECF 197-3, PageID 6932.)	***Response***: The City requests clarification as to the Team's source of disagreement. ***Rationale***: The City is unclear as to whether the Monitoring Team is rejecting 28 CFR 23 as the City's policy on criminal intelligence, or if the Team simply wants 28 CFR 23 clarified to include a statement that explains:	The City stands ready to address the Team's concern.	***Response***: After further discussion, the Team agrees with the City's proposal.	The Team does not recommend anything further.

	"In the event protected communications are intercepted, immediate notification, reporting, approval, and handling that will prevent political use and dissemination is required."			

Social Media Generally

Revised Policy Submitted To Court on 1/14/2019: Social media searches following a homicide or critical incident or occurrence of a crime should be limited to the social media accounts of persons who have been identified as suspects, victims, and/or witnesses to a crime. Only searches of open-sources (non-private) should be used.

City's Proposed Amendment to Revised Policy Submitted To Court on 1/14/2019: "If it becomes necessary to utilize an undercover social media account in the course of the criminal investigation, Director or Director's designee approval is required."

Scenario 4: May police officers review publicly accessible social media accounts (with either their personal PDA/phone or with a police-issued device) of victims, potential suspects, and witnesses as part of an active investigation into the planning or occurrence of a criminal act without Director approval pursuant to § G (e.g. a homicide scene and its immediate aftermath, such as where the responding officer searches Facebook for the name of the victim and/or the name(s) of any suspect(s))?

Team's Prior Feedback to City of Memphis	**City of Memphis's Response to Team's Prior Feedback**	**City of Memphis's Proposed Action in Response to Team's Prior Feedback**	**The Team's Response to the City's Proposed Action.**	**Recommendation(s)**
Regarding the	***Response***: The	The City	***Response***:	The Team

use of personal and police-issued devices, the Team disagreed that officers be able to use personal devices for work-related activities. Team expressed concern about the City's policy, or lack thereof, regarding the use of personal and police-issued devices. The Team recommended that the City restrict work-related social media searches to police-issued devices, unless there are extenuating circumstances, because the use of personal communication devices potentially implicates the First Amendment and Fourth Amendment rights of the officers who own the	City declines the Team's recommendation. ***Rationale***: The City believes that work-related business by officers, regardless of whether it is on police-issued devices or on personal communications devices, is generally subject to disclosure and review, and officers would not be able to object to access because of the mere fact that the work was performed on personal communications devices.	proposes amending its policy and procedures to clarify this issue.	The Team agrees that the City should amend its policy and procedures to reflect its position on police-issued and personal devices. In addition, the Team recommends language to accomplish this. ***Rationale:*** The proposed process would better facilitate internal and external audits.	recommends the following amendment: "All MPD personnel should only utilize Department-issued electronic devices when conducting official business on behalf of MPD. If, for any reason, an MPD officer or employee utilizes his or her personal electronic device when conducting official business, each search shall be documented and reported in a timely manner."

devices. (ECF 197-3, PageID 6930-6931.)				
The Team requested clarification about the scope of the searches that are covered by this policy. For example, the Team believed that searches of "witnesses" after the "occurrence of a crime" could sweep in a lot of information that's not related to the crime. Relatedly, the Team wanted to know whether these searches would only happen when there's reason to think that relevant information will be found on social media. (ECF 197-3, PageID 6931.)	***Response***: The City responds to the Team's request and declines its recommendation. The City states that the Social Media Policy covers all searches of social media done by any officer of the MPD. ***Rationale***: The City believes that it is a best practice to thoroughly search social media during a criminal investigation, even if those searches necessarily sweep in a lot of information that is unrelated to the crime. The City is willing to address the issue of how to handle this irrelevant information in its Social Media policy, but it does not believe pre-	None.	***Response***: The Team disagrees.	The Team submits that any MPD investigation that uses social media as an investigative technique must have a lawful purpose and must not unlawfully infringe the First Amendment Rights of the individual(s) or groups subject to the investigation—meaning, the social media investigation should employ the least intrusive means upon exercise of those First Amendment rights. Further, if the investigation infringes on First Amendment rights, then the authorization form and director's approval are required. Lastly, the Team reiterates the language of footnote 14 on page 34 of the Court's Order and Opinion, which is copied again here. "A police officer may, for example, need to 'friend' a suspected drug dealer as part of an investigation. The

	set parameters are practical or best practices.			officer in question would not be conducting political intelligence, because while he may incidentally obtain information relating to the suspect's exercise of First Amendment rights, he is not 'gathering' that information. This officer does, however, need to seek formal approval through use of the authorization form, because the investigation 'may result in the collection of information about the exercise of First Amendment rights.' (Consent Decree, at § G.)" Opinion And Order at p. 34 n.14 (Oct. 26, 2018) (ECF 151, PageID 6274 n.14.)

Criminal Intelligence

Proposed Policy: 28 CFR 23 in full.

Scenario 7: May the MPD investigate and monitor organized gangs reasonably suspected of involving criminal activity even though the right of association is protected by the First Amendment?

Team's Prior Feedback to City of Memphis	City of Memphis's Response to Team's Prior Feedback	City of Memphis's Proposed Action in Response to Team's Prior Feedback	The Team's Response to the City's Proposed Action.	Recommendation(s)
The Team	***Response***:	The City would	***Response:***	The Team does not

requested clarification about where the proposed language will be added. (ECF 197-3, PageID 6934.)	The City requests clarification about meaning of "proposed language." ***Rationale***: The City believes adopting 28 CFR 23's policy on criminal intelligence would address this scenario.	like to adopt 28 CFR 23's policy on criminal intelligence. The relevant portion of this section states, "A project shall not collect or maintain criminal intelligence information about the political, religious or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity." (§ 23.20(b))	The Team is satisfied with this explanation.	recommend anything further.

Crime Analysis and Reporting

<u>City's Current Policy</u>: MPD Real Time Crime Center Standard Operating Procedure (SOP).

"The RTCC will be the clearing house for gathering analytical data, as far as criminal activity, and processing the data into spread sheets, maps, or any array of information to be disseminated as needed throughout the MPD Command Staff and the MPD Public Information Officers. Civilian employees are responsible for specific daily statistics, which is covered in the CAU SOP." (§1.1.)

Scenario 8: May the MPD use information collected during the course of its investigations for the purpose of crime analysis and reporting? The central focus of crime analysis is the study of crime (e.g., rape, robbery, and burglary); disorder problems (e.g., noise complaints, burglar alarms, and suspicious activity); and information related to the nature of incidents, offenders, and victims or targets of crime (targets refer to inanimate objects, such as buildings or property). Crime analysis is also used for other police-related operational issues, such as staffing needs, addressing any deficiencies in training, and updating policies and procedures.

Team's Prior Feedback to City of Memphis	**City of Memphis's Response to Team's Prior Feedback**	**City of Memphis's Proposed Action in Response to Team's Prior Feedback**	**The Team's Response to the City's Proposed Action.**	**Recommendation(s)**
The Team recommended that the policy include language that makes it clear that "analytical data" does not include "political intelligence." After that, the policy should define "political intelligence." (ECF 197-3, PageID 6935.)	***Response***: The City accepts the Team's recommendation.	The City proposes adding the following language to paragraph 1.1.: "The RTCC will be the clearing house for gathering analytical data, as far as criminal activity, and processing the data into spread sheets, maps, or any array of	***Response:*** The Team agrees.	The Team does not recommend anything further.

		information to be disseminated as needed throughout the **MPD** Command Staff and the MPD Public Information Officers. Civilian employees are responsible for specific daily statistics, which is covered in the CAU SOP. **'Analytical data' shall not include political intelligence. 'Political Intelligence.' means the gathering, indexing, filing, maintenance, storage or dissemination of information, or any other investigative activity, relating to any person's beliefs, opinions, associations**		

		or other exercise of First Amendment rights."		
The Team recommended that the content of investigations and identities of non-charged persons—as well as their communications—should not be disseminated and noted that sharing information would likely violate the Consent Decree. (ECF 197-3, PageID 6935.)	***Response***: The City agrees with the recommendation and acknowledges that the sharing of information among law enforcement agencies may violate the Consent Decree. ***Rationale***: The City agrees that the sharing of such information among law enforcement agencies is likely prohibited by Section I of the Consent Decree "Restriction on Joint Operations." However, the City can contemplate situations during which it would be a matter of best police practices and in the best interest of public safety	The City proposes seeking clarification from the Court.	***Response:*** The Team would like examples of the types of situations during which it would be a matter of best police practices and in the best interest of public safety for law enforcement agencies to share information that would otherwise be impermissible under the Consent Decree.	The Monitoring Team maintains its original recommendation: The content of investigations and identities of non-charged persons—as well as their communications—should not be disseminated and noted that sharing information would likely violate the Consent Decree. (*See* ECF 197-3, PageID 6935.)

	for law enforcement agencies to share information that would otherwise be impermissible under the Consent Decree.			

Exigent Circumstances

City's Proposed Policy: An MPD officer may investigate or monitor a person who may be engaged in First Amendment activity without first obtaining the approval of the Director pursuant to § G under exigent circumstances. However, such an investigation must immediately be reviewed and authorized by the Director/Designee as soon as practicable for approval and documentation.

Scenario 9: May the MPD investigate or monitor a person engaged in First Amendment activity without first getting the approval of the Director pursuant to § G under exigent circumstances (e.g. searching the social media accounts of a person involved in organizing a gathering originally thought to be a protest, but that is quickly morphing into a riot/looting, for the purpose of determining where the crowd plans to go next)?

Team's Prior Feedback to City of Memphis	**City of Memphis's Response to Team's Prior Feedback**	**City of Memphis's Proposed Action in Response to Team's Prior Feedback**	**The Team's Response to the City's Proposed Action.**	**Recommendation(s)**
The Team recommended that it is reasonable to have an exigent circumstances policy; however, such a policy would require a modification of the Consent Decree. (ECF	***Response***: The City is unsure whether an exigent circumstances policy requires modification of the Consent Decree. ***Rationale***: The City does not	The City proposes taking this issue to the Court for clarification.	***Response:*** The Team agrees.	The Team does not recommend anything further.

197-3, PageID 6936.)	necessarily disagree with the Monitoring Team that an exigent circumstances policy requires modification of the Consent Decree. The City would propose taking this issue to the Court for clarification.			

Civilian Checkpoints

Current Policy: Civilian checkpoints — City Hall Lobby Entry and Garage Entry 1B

> Civilian checkpoints have been employed to monitor and control the movement of people and materials in order to prevent violence. All civilian entering City Hall shall be check and present valid photo identification and issued a visitor pass. Uniformed MPD officers are responsible for maintaining him/herself in a highly visible manner, deter crimes from happening on the property he/she is overseeing and ensure the people on the property are safe as well.

City's Proposed Civilian Checkpoint Policy:

> MPD may require visitors to City-owned buildings, including but not limited to City Hall and 170 North Main, to provide identification to gain entry to the building. MPD may require that all visitors be photographed and wear time-stamped identification badges while on City property. MPD may keep a log of all visitors to City buildings indefinitely. The practice of requiring identification, photographs, and a visitor's log is for the purpose of public and building safety, and is not for the purposes of political intelligence or interference with the exercise of First Amendment rights.

Scenario 10: May the City collect identifying information and photographs of all visitors to City Hall? A person attending a City Council meeting in City Hall is arguably exercising her First Amendment rights, and the photographing and documenting of that person by the commissioned MPD officers at the security desk could be construed by some as violating the Consent Decree.

Team's Prior Feedback to City of Memphis	City of Memphis's Response to Team's Prior Feedback	City of Memphis's Proposed Action in Response to Team's Prior Feedback	The Team's Response to the City's Proposed Action.	Recommendation(s)
The Team disagreed with the proposed policy and sought clarification about the City's security practices at City Hall. (ECF 197-3, PageID 6937.)	***Response***: The City responds to request for clarification and acknowledged the Team's concern. The City uses a system called LobbyGuard to track visitors to City Hall. Every visitor must show photo identification, which is scanned into the LobbyGuard software. The visitor is then photographed, and a label with the visitor's photo is printed out. This photo label must be worn by the visitor while in City Hall. The purpose of the photo is to ensure that the visitor is the person they	If the Monitoring Team feels that this term is too long, the City will address the issue with the vendor to see if the visitor logs and photographs can automatically delete after the designated period of time, as agreed upon by the Monitor.	***Response:*** The Team disagrees that the public should be required to take a photograph to enter City Hall: 1. the date when the City adopted its current photos-badges requirements; 2. a copy of the minutes of the City Council related to its adoption of this requirement and its approval of the contract with the vendor of the LobbyGuard system; 3. what other municipal buildings in addition to City Hall utilize the LobbyGuard system; and 4. the records	The Monitoring Team recommends the following: 1. The City and MPD may restrict access to "secure" areas inside City Hall as required to perform the business of the City. The Monitoring Team and the ACLU must agree with the City on the designation of "secure" areas. 2. Visitors to City Hall may be screened as required for legitimate safety and security purposes. 3. The least intrusive screening methods, such as metal detectors, should be used to enhance building safety and security. 4. Visitors entering City Hall shall not be required to show photo identification, provide their name or sign the visitor log

	purport to be. The photograph is intended to prevent such subterfuge. The vendor for the LobbyGuard system currently saves the photographs and visitor logs for a term of up to one year.		of the City showing the number of people who entered City Hall on an annual basis before and after the current system was adopted. ***Rationale***: The right of access to public areas, public governmental buildings, and public proceedings is protected by the First Amendment. ***Note***: The City responded to the Team's additional questions with the following: a. The system was installed in 2014. b. Adopting this process and contracting with LobbyGuard did not require City Council approval. c. 170 N. Main	unless their presence creates an actual or likely criminal law enforcement encounter. 5. Visitors may not be photographed in the absence of a legitimate, immediate law-enforcement predicate. 6. Visitors requiring access to "secure" areas of City Hall may be required to sign a visitor's log before gaining access. 7. Photographs and any information captured on the visitor log must be automatically deleted within fourteen (14) days absent a legitimate, continuing law-enforcement predicate, certified in writing.

			utilizes the LobbyGuard system. d. The City is not aware of existing records showing the number of people who entered City Hall prior to 2014. The current system can produce a list of persons entering City Hall. This list is only accessible to certain members of the City's Division of Information Systems. The City is not clear if this is a request for those records or just an inquiry generally, but it has attached the list that was previously provided to the ACLU. An updated list can be provided.	

Maintenance and Storage of Information Collected by MPD Cameras

City's Current Policy: MPD Real Time Crime Center Standard Operating Procedure (SOP). The relevant portion states:

> Video recorded by Blue Crush cameras are stored on the hard drive located within the camera enclosure. Recorded video of criminal activity is available for download through the client camera software or, in the event of software related issues, from the camera itself. The hard drive retains 30 days of video before it is overwritten. Video evidence not retrieved within 30 days will be lost.
>
> Upon written request from an investigative bureau, the associated video will be downloaded to DVD and given to the bureau detective for entry into their case as evidence.

(§ 1.6.)

Scenario 11: How should MPD handle the maintenance and storage of information collected by MPD cameras, such as SKYCOP cameras, building cameras, etc.?

Team's Prior Feedback to City of Memphis	**City of Memphis's Response to Team's Feedback**	**City of Memphis's Proposed Action in Response to Team's Feedback**	**The Team's Response to the City's Proposed Action.**	**Recommendation(s)**
The Team recommended adding the following language to the existing policy: "Upon written request from an investigative bureau, and approval by the Police Director or the Director's	***Response***: The City accepts the recommendations.	The City agrees to make the changes.	***Response:*** The Team agrees.	The Team does not recommend anything further.

Designee, the associated video will be downloaded to DVD or other portable media and given to the bureau for entry into their case as evidence. (§ 1.6.)" The Team further recommended changing "lost" to "destroyed." (ECF 197-3, PageID 6938.)				
The Team suggested that MPD's policies regarding the collection and dissemination of information may violate the Consent Decree. (ECF 197-3, PageID 6938-6939.)	***Response***: The City agrees with the Team's observation but states that it must be able to collect and maintain personal information about persons, even if they are not the subjects of lawful investigations. ***Rationale***: This is a matter of best police practices.	The City proposes taking this issue to the Court for clarification.	***Response:***	MPD's policies regarding the collection, maintenance, and storage of information may violate the consent decree. (*See* ECF 197-3, PageID 6938-6939.) Section C(1) of the consent decree prohibits the City from "engag[ing] in political intelligence," and section B(4) states that political intelligence includes "the gathering, indexing, filing, maintenance], [and] storage . . . of information . . . relating to any person's . . . exercise of First Amendment rights."

				The maintenance and storage of information collected by MPD's cameras, such as SKYCOP cameras, must therefore have a lawful purpose and be authorized and documented according to the protocols established by §§ G or H of the consent decree.

EXHIBIT B

BUTLER | SNOW

Confidential Attorney Work Product

M E M O R A N D U M

To: The City of Memphis

From: Independent Monitor Edward L. Stanton III

Date: August 21, 2019

THE INDEPENDENT MONITOR'S RESPONSES TO QUESTIONS REGARDING POTENTIAL COORDINATION BETWEEN THE MEMPHIS POLICE DEPARTMENT, OTHER LAW ENFORCEMENT AGENCIES, AND NON-LAW ENFORCEMENT ENTITIES AND INDIVIDUALS

This memorandum addresses three questions concerning the City of Memphis (City) and the Memphis Police Department (MPD)'s ability to share with and receive information from other law enforcement agencies.

(1) On September 9-11, 2019, the City will host the PSP Symposium on Violent Crime. U.S. Attorney General William Barr and executives from various federal agencies—DOJ, FBI, DEA, ATF, and USMS—plan to attend. On July 16, 2019, the City asked whether it may "coordinate with [the FBI and Secret Service] and benefit from Intel they may have to share in planning for th[e] symposium." (*See* Email from B. McMullen to E. Stanton, et al., attached as **Exhibit A**.)

ANSWER: This question raises two issues: First, to the extent that "coordinat[ing]" with the FBI or the Secret Service includes sharing personal information, the City may not coordinate with those agencies, or any others, in planning for the symposium. Section H of the *Kendrick* Consent Decree[1] prohibits the City from "maintain[ing] personal information about any person unless it is collected in the course of a lawful investigation of criminal conduct." § H(1). It also prohibits the City from sharing "personal information . . . collected in the course of a lawful investigation of criminal conduct" unless the recipient is "another governmental law enforcement agency then engaged in a lawful investigation of criminal conduct." § H(2). I read this language to impose two applicable restrictions: (1) entirely against the sharing of personal information collected in any way other than via lawful criminal investigation (as such information may not be maintained in the first instance); and (2) against the sharing of personal information collected via lawful criminal investigation unless such sharing is with another governmental law enforcement agency and that agency already is engaged in a lawful criminal investigation.

---

[1] The decree is ECF No. 3 in Case No. 2:76-cv-000449 before this Court.

The second restriction is straightforward, but the first warrants elaboration. As an initial matter, § C(1) of the consent decree broadly prohibits the City from "engag[ing] in political intelligence." Section B(4) defines "political intelligence" to include both "the gathering [and] . . . dissemination of information . . . relating to any person's . . . exercise of First Amendment rights." Together, the two provisions prevent the City from sharing information relating to any person's exercise of First Amendment rights.

Section H(2), cited above, is broader than Section B(4). It speaks of "personal information" without qualification, whereas § B(4) refers to the narrower category of "information . . . relating to any person's . . . exercise of First Amendment rights." But § H(2) restricts the permitted recipients of the first category of information to other "governmental law enforcement agenc[ies] then engaged in a lawful investigation of criminal conduct" when that information is acquired "in the course of a lawful investigation of criminal conduct." If personal information is collected in some way other than via lawful criminal investigation, then § H(2)'s prohibition does not reach it. And if personal information does not relate to the exercise of a person's First Amendment rights, then §§ B(4) and C(1)'s prohibition does not reach it either.

Thus, §§ B(4), C(1), and H(2), which prohibit outright or limit the sharing of two categories of information, implicitly allow the City freely to share a third category: (1) personal information, (2) not collected in the course of a lawful criminal investigation, that (3) does not relate to any person's exercise of First Amendment rights.

But § H(1) eliminates this third category. Like § H(2), § H(1) refers broadly to "personal information" without qualification. And it prohibits the City from "maintain[ing] personal information about any person unless it is collected in the course of a lawful investigation of criminal conduct and is relevant to such investigation" (emphasis added). If personal information does not satisfy both criteria, then § H(1) states that it "shall be destroyed." As a result, if the City were to identify information that fell within this third category, then it could not share that information because § H(1) would not allow the City to keep it in the first place.

The ultimate consequence of these four sections, B(4), C(1), H(1), and H(2), is that the City may collect personal information—related or unrelated to the exercise of First Amendment rights—only in the course of a lawful criminal investigation, and may share that information only with a governmental law enforcement agency that already is involved in a criminal investigation.

Second, the City may not "benefit from the Intel" acquired by the FBI, the Secret Service, or any other law enforcement agencies unless the City first verifies that the information was not acquired in any way that the consent decree prohibits the City from using. Section I of the *Kendrick* Consent Decree forbids the City to "encourage, cooperate with, delegate, employ or contract with, or act at the behest of, any local, state, federal or private agency, or any person, to plan or conduct any . . . activity . . . prohibited by th[e] decree." I read this restriction to place the onus on the City to verify that any information it receives from governmental law enforcement

agencies, non-law enforcement agencies, public and private entities, and individuals satisfies the same standards as information lawfully collected by the City itself.

> **(2)** The City previously has "expressed concern that the [*Kendrick*] Consent Decree might prohibit the City from receiving intelligence collected by other law enforcement agencies, *e.g.* Shelby County Sherriff's Department, TBI, or FBI, that would otherwise be prohibited by the Consent Decree if obtained by the MPD." (*See* June 14, 2019, Letter from M. Glover to E. Stanton, attached as **Exhibit B**, at 2.) "[O]ther law enforcement agencies," the City explained, "are not bound by the Consent Decree [and] might obtain criminal intelligence through methods for which the MPD is prohibited from using under the Consent Decree." (*Ibid.*) "The City wants to make sure that its receipt of such information from other law enforcement agencies does not violate the Consent Decree." (*Ibid.*)

ANSWER: The City's receipt of intelligence collected by the Shelby County Sherriff's Department, the TBI, the FBI, or other law enforcement agencies would violate the consent decree unless the City first verified that the information was not acquired in any way that the consent decree prohibits, as explained in the second section of my response to the first question above. In responding to this inquiry on a conference call on June 14, 2019, I stated that the City's receipt of such intelligence would not violate the consent decree. Upon further review of the consent decree and the court's orders in this litigation, I continue to believe that this answer is correct—but only so long as all intelligence properly is verified before the City receives it. If intelligence collected by governmental law enforcement agencies is not verified before the City receives it, then the City's receipt of that intelligence would violate the consent decree. Moreover, if the City receives criminal intelligence from a governmental law enforcement agency for the purpose of conducting or supervising the MPD's own investigation of criminal conduct, then the City's receipt of that information also may be subject to the authorization and reporting requirements of § G of the consent decree.[2]

---

[2] Section G of the *Kendrick* Consent Decree states:

> 1. Any police officer conducting or supervising a lawful investigation of criminal conduct which investigation may result in the collection of information about the exercise of First Amendment rights, or interfere in any way with the exercise of such First Amendment rights, must immediately bring such investigation to the attention of the Memphis Director of Police for review and authorization.
>
> 2. The Director of Police shall review the factual basis for the investigation and the investigative techniques to be employed. The Director of Police shall issue a written authorization for an investigation for a period not to

Please either (1) confirm that the City has not received intelligence collected by governmental law enforcement agencies without first verifying that information as provided above or (2) identify all unverified information that the City has received from governmental law enforcement agencies from June 14, 2019, to the date of this correspondence.

(3) The City also has asked whether it may "share intelligence about a possible First Amendment Event that might end up on or near, for example, the campus of St. Jude or FedEx Headquarters." (**Ex. B** at 2-3.)

ANSWER: The sharing of personal information with non-law enforcement entities was a specific subject of the court's attention when it held last October that the City had violated the consent decree. (*See* ECF No. 151, PageID # 6268-69.) In a section entitled, "The City Violated the Consent Decree by Disseminating Information Related to First Amendment Rights to Outsiders," the court observed that the City's Office of Homeland Security had "shared personal information [collected in the course of a criminal investigation] with certain outside individuals, including Autozone's Head of Security, upon request and supervisor approval." (*Ibid*.) In an earlier order in August 2018, the court explained that the MPD had shared joint intelligence briefings (JIBs) with "regional law enforcement officials and certain members of the Memphis community . . . employees of the U.S. Department of Justice . . . [and] Shelby County Schools,

---

exceed ninety (90) days only if the Director of Police makes written findings that:

a. The investigation does not violate the provisions of this decree; and

b. The expected collection of information about, or interference with, First Amendment rights is unavoidably necessary for the proper conduct of the investigation; and

c. Every reasonable precaution has been employed to minimize the collection of information about, or interference with, First Amendment rights; and

d. The investigation employs the least intrusive techniques necessary to obtain the information.

3. The Director of Police may authorize an extension of such investigation for an additional period specified by the Director of Police not to exceed 90 days. The Director of Police shall authorize each such an extension only if the Director of Police re-evaluates the factual basis for the investigation and investigative techniques to be employed, and makes current written findings as required in paragraph 2, above.

FedEx, AutoZone, and St. Jude." (ECF No. 120, PageID # 4865 (emphasis added).) The court ultimately concluded that the City had "violated Section C(1) of the Consent Decree"[3] by sharing JIBs in this way. (*Id.* at PageID 4880, 4881.) It also identified § H(2), which applies to personal information collected in the course of a criminal investigation and is referenced above in my response to the City's first question, as an additional limitation on sharing "information . . . relating to any person's beliefs, opinions, associations or other exercise of First Amendment rights." (Consent Decree § B(4); *see* ECF No. 151, PageID # 6268.)

In responding to this inquiry on a conference call on June 14, 2019, Deputy Monitor Jim Letten stated that the Monitoring Team would need to analyze the inquiry under the consent decree "and suggested that the sharing of intelligence with a quasi-law enforcement agency, such as the security force at St. Jude, might be permissible under the Consent Decree." (**Ex. B** at 3.) Upon review of the consent decree and later orders of the court in this litigation, it is my view that the City may not share political intelligence with non- or quasi-law enforcement agencies under any circumstances. As discussed in the first section of my response to the City's first question above, I read §§ B(4), C(1), H(1), and H(2) of the consent decree to prohibit entirely the sharing of personal information collected in any way other than via lawful criminal investigation. We also read those sections to prohibit the sharing of personal information collected via lawful criminal investigation unless such sharing is with another law enforcement agency and that agency already is engaged in a lawful criminal investigation.

I discern no public-safety or quasi-law enforcement exceptions to these prohibitions in either the plain language of the consent decree or the court's orders in this litigation.

[3] Section C(1) of the *Kendrick* Consent Decree states: "The defendants and the City of Memphis shall not engage in political intelligence."

Exhibit A

Bethany Pollock

From: McMullen, Bruce <Bruce.McMullen1@memphistn.gov>
Sent: Tuesday, July 16, 2019 8:13 PM
To: Edward L. Stanton III
Cc: Jill Silk; Shanell Tyler; Will Perry; Glover, R. Mark; Tullis, Mary Wu; McMullen, Bruce; Sink, Jennifer
Subject: Re: Upcoming event.

Ed and Will,

We are hosting the 2019 PSP Symposium on Violent Crime (September 9-11). Attorney General William Barr plans to attend as well as executives from the DOJ, FBI, DEA, ATF, and USMS.

Behind the scenes:

1. MPD will be responsible for event security; 5-6 officers each day inside the hotel and additional officers in the parking lot area.

2. MPD will need to provide executive protection on day one with AG Barr. Barr's advance team will arrive the Friday before, on September 6, 2019.

3. MPD will need to coordinate an evening of entertainment and tour of selected MPD facility. Typically Tuesday night. Most Likely RTCC or CGIC and a night on Beale. For 350 attendees, this could mean 6 buses.

We anticipate the need for a lot of coordination with the various agencies. Because of those involved, we expect the FBI and Secret Service to have a security force on the ground (or the air, I don't know the extent of their technology). As you may expect, the expectation is that the agencies will share intelligence with MPD, and they expect the same. The intel they share with MPD may be obtained through methods that are prohibited by the Consent Decree. We would like to know if we have your approval to coordinate with these agencies and benefit from Intel they may have to share in planning for this symposium.

Sent from my iPhone

On Jul 16, 2019, at 6:26 PM, Edward L. Stanton III <Edward.Stanton@butlersnow.com> wrote:

Bruce —

Let's plan to discuss on our call Friday.

ELS

Sent from my iPhone

On Jul 16, 2019, at 6:08 PM, McMullen, Bruce <Bruce.McMullen1@memphistn.gov> wrote:

Ed and Will,

Since we did not get a response with respect to the use of these search terms before the Nathan Bedford rally Saturday at Health Science park, we did not use them. Thankfully, the crowd was in line with what the permit suggested and there was no incident.

Bruce McMullen
Chief Legal Officer/City Attorney
125 N. Main, Room 336
Memphis, Tennessee 38103
(901) 576-6614 – Office
(901) 576-6531 – Fax
bruce.mcmullen1@memphistn.gov

From: Silk, Jennie [mailto:jsilk@bakerdonelson.com]
Sent: Friday, July 12, 2019 5:06 PM
To: Edward L. Stanton III
Cc: Shanell Tyler; Will William Perry (will.perry@butlersnow.com); Glover, R. Mark; Tullis, Mary Wu; McMullen, Bruce; McMullen, Bruce
Subject: RE: Search terms for Nathan Bedford Forrest Birthday Rally and Confirming Use of Cameras at Rally Tonight

Apologies, but we would like to add the following search terms to the original list below:
Proud Boys
Garvin McInnes
unite the white
Richard Spencer
Jason Kessler

Thank you,

Jennie Vee Silk
Associate
Baker, Donelson, Bearman, Caldwell & Berkowitz, PC
2000 First Tennessee Building
165 Madison Avenue
Memphis, TN 38103
Phone 901.577.8212
Fax 901.577.0812
JSilk@bakerdonelson.com

From: Silk, Jennie
Sent: Friday, July 12, 2019 4:41 PM
To: Edward L. Stanton III
Cc: 'Shanell Tyler'; Will William Perry (will.perry@butlersnow.com); Glover, R. Mark; Tullis, Mary Wu; 'McMullen, Bruce'; McMullen, Bruce
Subject: Search terms for Nathan Bedford Forrest Birthday Rally and Confirming Use of Cameras at Rally Tonight

Hi Ed,

As we discussed on the call today, a rally is planned this weekend to celebrate Nathan Bedford Forrest's birthday, which is tomorrow July 13. You instructed the City to send you the search terms that MPD needs to search on social media in order to adequately prepare for this event. Here is the list:

Confederate
NBF

Forrest
July 13
July 13, 1821
October 29
October 29, 1877
Statue
December 20, 2017
Sons of the Confederacy
SOC
Nathan Bedford Forrest
Friends of Nathan Bedford Forrest
Confederate901
Confederate 901
Taking Our Country Back
Hiwayman Operation Home Front
highwaymen
Rollin Memphis
KKK
Ku Klux Klan
Grand Wizard
Health Sciences Park
Lee Millar
Calvary General
Battle of Fort Pillow
Battle of Shiloh
Confederate Hero
Battle of Fort Donelson
Battle of Tupelo
KKK
Billy Roper
Shield Wall

<u>Possible Counter protesters:</u>

CCC
Coalition of Concerned Citizens
New Black Panthers
Antifa

Please understand that we are very sensitive to the issue of the counter-protester group names listed above, however, the City needs to prepare for the possibility of a large counter protest that could turn violent or become otherwise disruptive. As you know, whenever two ideologically opposite groups converge, things could erupt, similar to what happened in Charlottesville, Virginia.

This note also confirms that today the Monitoring team gave the City the greenlight to operate its SkyCops, Body Worn Cameras, and Dash Cams pursuant to the current MPD policy for each of those cameras at the rally planned for tonight centered on the release of journalist Manuel Duran from ICE custody.

Please let us know if you have any questions or concerns. Thank you and the team for taking the time to address these issues on the call today.

Best,

Jennie Vee Silk
Associate

Baker, Donelson, Bearman, Caldwell & Berkowitz, PC
2000 First Tennessee Building
165 Madison Avenue
Memphis, TN 38103
Phone 901.577.8212
Fax 901.577.0812
JSilk@bakerdonelson.com

Exhibit B

BAKER DONELSON
BEARMAN, CALDWELL & BERKOWITZ, PC

2000 FIRST TENNESSEE BUILDING
165 MADISON AVENUE
MEMPHIS, TENNESSEE 38103

PHONE: 901.526.2000
FAX: 901.577.2303

www.bakerdonelson.com

R. MARK GLOVER
Direct Dial: 901.577.2222
Direct Fax: 901.577.0732
E-Mail Address: mglover@bakerdonelson.com

June 14, 2019

Ed Stanton
Butler Snow
6075 Poplar Avenue, Suite 500
Memphis, TN 38119
Edward.stanton@butlersnow.com

Re: June 14, 2019 Conference Call Recap

Ed,

This letter is intended to recap and memorialize several points from our conversation this morning on the conference call between you, members of your team, and the City's attorneys. Thank you for your prompt attention to the issues and your willingness to provide guidance.

The City's Request for a Real-Time Response Procedure

The City requested a procedure for obtaining a "real time" response from the Monitor on questions or issues that might arise that require immediate guidance.

You recommended that the procedure for the City to obtain an immediate response from the Monitor is first to send an email outlining the issue or question to you, Jim Letten, and Will Perry. If no one responds after a short period of time, you requested that a member of the City's legal team then call the cell phone of you, Jim, or Will to follow up on the initial email. Shanell has since provided the City with the relevant cell phone numbers.

It was then decided that for more long-range requests, a member of the City's legal team will email such a request to you, Jim, and Will and await a response.

Body Worn Cameras at Community Engagement Event

The City sought clarification on whether an MPD officer attending the upcoming Community Engagement Event should turn off his/her body worn camera ("BWC") while in the event. Bruce explained that the BWCs have three states: off, sleep, and recording. When the BWC is in the sleep mode, it is recording, but the footage is not retained unless and until the officer activates the BWC to record. Once activated, the BWC goes back and retains the prior 30 seconds of footage just before the BWC's activation. The City further explained that there are also several "triggering events" such as gunshots, sirens, etc. that will cause all the BWCs in the vicinity to start recording, without officer activation.

You recommended that the BWCs remain in sleep mode at the Community Engagement event, pursuant to the current MPD policy.

Interim Authorization Form

The City requested that you approve the use of an Interim Authorization Form. We emailed to you a draft of that Interim Authorization Form earlier this afternoon, per your request.

Please let us know as soon as possible if the Interim Authorization Form is acceptable to use until the Court approves the final Authorization Form. In the event that the Director must authorize an investigation before your team has a chance to review and approve the Interim Authorization Form, the City will just use the Interim Form. You stated that was acceptable to you based upon the events of the past few days.

Sharing of Information with Other Law Enforcement Agencies

The City expressed concern that the Consent Decree might prohibit the City from receiving intelligence collected by other law enforcement agencies, *e.g.* Shelby County Sherriff's Department, TBI, or FBI, that would otherwise be prohibited by the Consent Decree if obtained by the MPD. The City explained that other law enforcement agencies that are not bound by the Consent Decree might obtain criminal intelligence through methods for which the MPD is prohibited from using under the Consent Decree. The City wants to make sure that its receipt of such information from other law enforcement agencies does not violate the Consent Decree.

You stated unequivocally that, according to your understanding, the City's receipt of such information does not violate the Consent Decree.

Sharing of Information with Non-Law Enforcement Agencies

I posed the question concerning whether the City would be allowed to share intelligence about a possible First Amendment event that might end up on or near, for example, the campus of St. Jude or FedEx Headquarters. Jim Letten explained that your team would need to analyze that under the Consent Decree, and suggested that the sharing of intelligence with a quasi-law

enforcement agency, such as the security force at St. Jude, might be permissible under the Consent Decree, and he understands the public safety purpose.

In the interim, should such a situation arise, the City will use the Real Time Response procedure outlined above to seek your team's authorization.

The City appreciates your team's recognition of the importance of public safety, and your willingness to make decisions in real time. Thank you for your continued guidance.

Best regards,

BAKER, DONELSON, BEARMAN,
CALDWELL & BERKOWITZ, PC

R. Mark Glover

cc: Will Perry
Jim Letten
Shanell Tyler
Jennie Silk
Mary Tullis

EXHIBIT C

BUTLER | SNOW

August 26, 2019

VIA ELECTRONIC MAIL

R. Mark Glover, Esq.
Baker Donelson
Bearman, Caldwell & Berkowitz, PC
2000 First Tennessee Building
165 Madison Ave.
Memphis, TN 38103

Re: *ACLU-TN v. City of Memphis*, Case No. 2:17-cv-02120-JPM-jay:
The Monitoring Team's Responses to the City's outstanding RFAs.

Dear Mark:

On Wednesday, August 7, 2019, the court docketed the Monitoring Team's Second Quarterly (Q2) Report and made the report available to the City and the ACLU-TN.[1] (*See* Sealed ECF No. 218.) On Monday, August 12, 2019, the Monitoring Team responded to the City's letter of June 7, 2019, which addressed the City's remaining questions regarding the sufficiency of its January 14, 2019, submissions to the court (*see* ECF Nos. 183, 185) and proposed protocols for the eleven hypothetical scenarios submitted to the Monitoring Team in March (*see* Sealed ECF No. 197-3). The August 12 response mentioned that the discrete requests for authorization (RFAs) raised by the City would be addressed in separate correspondence.

This letter is the second of two correspondences that address the City's RFAs. The first, a memorandum opinion provided to the City on August 21, 2019, addressed RFAs related to the Memphis Police Department (MPD)'s ability to share and receive personal information with other law enforcement entities and non-law enforcement entities and people (Coordination Opinion). This letter both addresses certain questions of the Monitoring Team regarding the RFAs to which I responded before the submission of the Q2 Report and also responds to the RFAs, other than those addressed by the Coordination Opinion, that the City has raised since the submission of the Q2 Report. Related to the prior RFAs is a July 19, 2019, disclosure by the City that concerns the use of imposter accounts on Facebook. This letter also addresses that disclosure.

---

[1] The Monitoring Team submitted the Q2 Report to the court on Wednesday, July 24, 2019, without one of the report's exhibits—Exhibit 4, the Monitoring Team's proposed Audit & Compliance Plan for the Memphis Police Department. The court then ordered the Monitoring Team to submit the plan by August 2, 2019 (*see* ECF No. 216), which it did.

Post Office Box 171443
Memphis, TN 38187-1443

EDWARD L. STANTON III
901.680.7369
edward.stanton@butlersnow.com

Crescent Center
6075 Poplar Avenue, Suite 500
Memphis, TN 38119

T 901.680.7200 • F 901.680.7201 • www.butlersnow.com

BUTLER SNOW LLP

I.
Questions Regarding Prior RFAs.

In the Q2 Report (Sealed ECF No. 218), the Monitoring Team highlighted three RFAs by the City to which I had then responded, based on my authority qua "special master" to approve or prohibit certain conduct. (*See* Hr'g Tr., ECF No. 207, PageID # 7189: 16-25.) I responded to those RFAs on May 9, 2019; June 12, 2019; and July 12, 2019. (*See* Sealed ECF No. 218, PageID # 7395.) The Q2 Report also explained that the Monitoring Team was "pursuing additional information related to a July 19, 2019, disclosure by the City related to the use of Facebook." (*Id.* at PageID # 7390 n. 7.) The questions raised in this section concern the second and third RFAs and the July 19, 2019, disclosure.

A. June 12, 2019, RFA.

At 11:49 P.M. on June 12, 2019, City Attorney Bruce McMullen requested authority to access the Facebook accounts of Memphis residents for "a situation in North Memphis and a crowd out of control." (Sealed ECF No. 214, Ex. 2.) Mr. McMullen explained that "[t]here was chatter on social media" but that the MPD was "in the blind" and could "only use what people t[old] [them]." (*Ibid.*) He asked to "monitor social media"—specifically "identi[ying] Facebook accounts"—and to use "unidentified accounts" because one suspect was dead, another on the run, and the MPD was "facing a possible reprise of the crowd but d[idn't] know what [the crowd] w[as] planning." (*Ibid.*) I approved Mr. McMullen's RFA 35 minutes later, at 12:24 A.M. (*Ibid.*)

On July 16, 2019, in its quarterly filing regarding the MPD's use of social media searches, the City elaborated on this RFA, which occurred "in the aftermath of the US Marshal-involved shooting of Mr. Brandon Webber." (*Id.* at 3.) According to the City, "the vast majority of the individuals on this list of search terms were not associated with a protest or other scenario in which First Amendment rights were being exercised," but "four individuals listed were present at the scene" of the June 12 incident. (*Ibid.*) "Those persons were Chris Long, Frank Gotti (Gibson), Keedran Franklin, and Derrion Childs."[2] (*Id.* at 4.)

The Monitoring Team has questions related to four aspects of this quarterly filing, the social-media searches that the City conducted related to the June 12 incident, and the City's gathering, maintenance, and reporting of information about those searches:

- ***First***, the City identified in its quarterly filing certain limitations in its ability to report the social-media searches conducted by MPD officers as ordered by the court. According to the City, compliance with the court's orders "must rely in large part on self-reporting by . . . MPD officers." (*Id.* at 2.) "Even where social media use occurs

---

[2] Mr. Franklin, of course, was one of the original plaintiffs in this lawsuit; he and Mr. Gotti actively have been following this case and attended the Community Forum on July 11, 2019. *See, e.g.*, "Team Monitoring MPD Conduct to Speak at Public Forum," on local Channel 3 (link available here).

on the City's network," the City explained further, "some social media sources require an individual account to access content, but others do not, so only those requiring an individual account would presumably have search history that is traceable to that user." (*Ibid.*)

- Please identify which social media platforms used by MPD officers in connection with their official duties require an individual account to access content and which do not.

- Does the City have any generic accounts on any social media platforms that officers may use in connection with their official duties? If so, then is there a log or other documentation that establishes who uses those accounts and the dates and times of that use?

- Please confirm that searches that occur via any generic social media accounts operated by the City are being included in the City's quarterly reports to the court irrespective of whether those searches can be linked to specific users.

- Please state whether all social media searches that occur on the City's network can be linked to specific users. If not, then please explain why.

- Please also confirm that searches that occur on the City's network are being included in the City's quarterly reports to the court irrespective of whether those searches can be linked to specific users.

- ***Second***, in future quarterly reports, please add officers detailed to the Multi-Agency Gang Unit to the groups of officers ordered to report all search terms entered by them into social media sites to collect information for the purpose of conducting police business. The current list of officers as reported by the City includes officers detailed to the Office of Homeland Security, the Real Time Crime Center, the General Investigative Unit, Homicide, the Sex Crimes Unit, and members of Command Staff (Listed Officers). (*See ibid.*)

- ***Third***, in describing the written instructions that Listed Officers receive, the City stated that the instructions are accompanied by reference guides on how to collect individual search history on the commonly used social media sources—Facebook, Instagram, and Twitter. (*Ibid.*) Please confirm whether officers' social media use is limited to these three platforms. If not, then please identify the additional platforms and include reference guides regarding the same with instructions to officers about reporting social media search terms.

- ***Fourth***, the City stated that "Colonel Greg Sanders first viewed the publicly-available Facebook feeds of [Long, Gotti, Franklin, and Childs], . . . identified video containing evidence of . . . assaults and vandalism, and . . . instructed Sergeant Filsinger to obtain a search warrant for video footage of the events that evening." (*Id.* at 4.)

- Did Col. Sanders or Sgt. Filsinger complete an authorization form contemplated by § G of the consent decree and otherwise document this investigation as contemplated by § G?[3]

- Were "unidentified" or imposter accounts, on Facebook or other social media platforms, used by MPD in connection with this investigation?

- How many MPD imposter accounts, if any, have remained active since deactivation of the "Bob Smith" Facebook account referenced in this litigation?[4]

- Are the social media searches done via any such imposter accounts being included in the City's quarterly reports to the court?

B. July 12, 2019, RFA.

On July 12, 2019, the City made two, related requests of the Monitoring Team. First, the City requested permission "to operate its SkyCops, Body Worn Cameras [BWCs], and Dash Cams pursuant to the current MPD policy for each of those cameras at [a] rally planned for [that evening] centered on the release of journalist Manuel Duran from Ice Custody." (Email from J. Silk to E. Stanton, attached as **Ex. 1**.) Second, the City asked to used certain search terms on social media to prepare for "a rally . . . to celebrate Nathan Bedford Forrest's birthday, which [wa]s [Saturday] July 13." (*Ibid.*) The search terms included several "counter-protester group names," including the Coalition of Concerned Citizens, to which the City explained that it was "very sensitive." The Monitoring Team reviewed, but did not authorize, the proposed social media search terms. The City since has confirmed that it did not use any of the terms and that the rally went off without incident.

After a conference call with the City's legal counsel that lasted about an hour—the full Monitoring Team was still in Memphis, having assembled for the first Community Forum on July 11, 2019, and was able to deliberate contemporaneously—I granted the first request. The grant was premised on the understandings that the BWCs would not continuously record—they would instead record only when specifically activated by an officer and would then capture a 30-second "buffer" prior to activation—and that SkyCop and Dash Cam data would not be maintained or indexed without a § G authorization.

This request raises some concerns because it appears not to have been based on accurate information. After the Monitoring Team's conference call with the City's legal counsel on July

---

[3] I realize that an Interim Authorization Form for use in § G investigations was approved by the Monitoring Team after June 12, 2019. I'd like to know what, if any, documentation the City used before that form was approved.

[4] The Monitoring Team has raised this question before. Please see § I(C) & n. 5, *infra*.

12, 2019, Audit and Compliance Expert Dave McGriff followed up via phone with MPD Deputy Chief Don Crowe to ask about the particulars of the MPD's planned response to the Duran rally that evening. Chief Crowe informed Mr. McGriff that the MPD had planned no response to the rally due to the small number of anticipated protestors and that there would not be any uniform officers on the scene. Chief Crowe also advised Mr. McGriff that there were no stationary SkyCop cameras near the rally site (80 Monroe).

This information is inconsistent with the RFA that the Monitoring Team received earlier in the day. In a subsequent weekly conference call with the City's legal counsel, Mr. McMullen apologized for the error, explaining that there had been some miscommunication between himself and the MPD about the Duran rally and that his information was incorrect. It should go without saying that it is imperative for all RFAs to be verified before they are directed to the Monitoring Team.

C. July 19, 2019, Disclosure.

In the Monitoring Team's Q2 Report, we noted that "community members are aware that the MPD's use of the 'Bob Smith' account was held by the [c]ourt to violate the *Kendrick* Consent Decree, but also understand that several other undercover accounts improperly being used by the City were disabled." (Sealed ECF No. 218, PageID # 7398.) We also noted that we were "pursuing additional information related to a July 19, 2019, disclosure by the City" that implicated these concerns. (*Id.* at PageID # 7390 n. 7.)

The July 19, 2019, disclosure included two sets of correspondence between Mr. McMullen and Facebook.[5] (*See* Email & attachments from B. McMullen to E. Stanton, attached as **Exhibit 2**.) The first set of correspondence, which occurred in October 2016, concerned several imposter accounts that had been created on Facebook to impersonate Memphis Mayor Jim Strickland and his wife.[6] The second set, relevant here, occurred in September and October 2018, between the court's August and October 2018 orders holding that the City had violated the consent decree. (*See* ECF Nos. 120 & 151 / 152.) It concerned the MPD's creation and use of imposter accounts and was initiated by Facebook Director and Associate General Counsel for Security Andrea Kirkpatrick. (*See* Second and Third Attachments, **Ex. 2**.)

In September 2018, Ms. Kirkpatrick wrote to MPD Director Michael Rallings, explaining that she "recently [had] learned through media reports and the Electronic Frontier Foundation (EFF) that the [MPD] created fake Facebook accounts and impersonated legitimate Facebook

---

[5] Earlier that day, on the Monitoring Team's weekly call with the City, I first raised community concerns about imposter accounts other than the "Bob Smith" account.

[6] According to the City, the imposter accounts were "misleading and pose[d] a threat to public safety." (Email of October 28, 2016 at 12:32 PM, from B. McMullen to records@facebook.com, First Attachment, **Ex. 2**.) Coordinating with the FBI, it appears that the City was able to get Facebook to shut down these imposter accounts. (*See generally* First Attachment, **Ex. 2**.)

users as part of its investigation of alleged criminal conduct unrelated to Facebook." (Second Attachment, **Ex. 2**.) She stated that such imposter accounts "violate[] [Facebook's] terms of service" and requested that the MPD, "its members, and any others acting on its behalf cease all activities on Facebook that involve impersonation or that otherwise violate [Facebook's] policies." (*Ibid.*)

After verifying the authenticity of the letter, Mr. McMullen requested information about "6 additional accounts [other than the "Bob Smith" account]," explaining that he understood "from unconfirmed press reports" that Facebook had identified those accounts as being "associated with MPD's account." (*Ibid.*) Ms. Kirkpatrick responded that Facebook had taken action on six accounts that "were forensically related to the 'Bob Smith' account," ultimately checkpointing, authenticating, and reactivating three of the accounts and disabling the other three as fake. (*Ibid.*) She provided Mr. McMullen the URLs for the fake accounts and referred the City to Facebook's Law Enforcement Guidelines for additional information. (*Ibid.*)

The City's July 19, 2019, disclosure also included a third set of correspondence, internal to the City. (*See* Third Attachment, **Ex. 2**.) In that correspondence, City employee Michael Rodriguez explained to Mr. McMullen that no forensic analysis of the three fake accounts was possible because those accounts had been deactivated. (*Ibid.*) Mr. Rodriguez also stated that, to be "forensically related" to the "Bob Smith" account, the additional accounts had to have similar associated data—"[P]erhaps the same computer was used to create the account[s], the same user id was used to create the account[s] . . . A MAC address or IP address across the urls was related." (*Ibid.*)

Despite these correspondences, it is not clear from the July 19, 2019, disclosure whether the MPD has operated or is operating imposter accounts other than the "Bob Smith" account or, if so, whether Facebook is the only platform on which MPD has used imposter accounts. In his cover email describing the disclosure, Mr. McMullen stated that the City "investigated but had no knowledge of any other imposter accounts other than 'Bob Smith.'" (**Ex. 2**.) Please provide whatever information the City has in its possession, custody, or control regarding the three accounts disabled by Facebook as fake. Please also provide the related information sought by the final three questions in the fourth area of inquiry in § I(A), above.

II.
Responses to Outstanding RFAs.

Aside from an RFA on July 16, 2019, and related inquiries on June 7, 2019, all of which were addressed in the August 21, 2019, Coordination Opinion, the City has directed five RFAs to the Monitoring Team since the submission of the Q2 Report—on July 26, 2019; July 29, 2019; August 5, 2019; August 22, 2019; and August 23, 2019. This section addresses each request.

A. July 26, 2019, RFA.

During a weekly conference call with the City's legal counsel on Friday, July 26, 2019, the City asked whether City representatives would be allowed to attend planned focus groups

(*see, e.g.*, Joint Public Engagement Plan, ECF No. 211, PageID # 7282) as they are scheduled.[7] According to the City, it does not want to participate in the focus groups, but wishes merely to "observe" them, and focus group participants need not be informed that representatives of the City are present. To that end, the City offered to send officers in plain clothes to observe the focus groups and suggested that the officers refrain from identifying themselves.[8]

This request is denied in the strongest possible terms. At best, the request is tone deaf: "May the City secretly monitor Memphis residents during focus groups about the City's secret (and unlawful) monitoring of Memphis residents?" At worst, it is Orwellian: If granted, the request would convert a mechanism for vindicating individual rights into a device for degrading and invading those same rights—all in the guise of promoting them. Understood either way, the request undermines the court's impressions that the City's prior violations of the *Kendrick* Consent Decree "stem from a shared misunderstanding of the Decree's requirements, rather than political favoritism" (Order, ECF No. 151, PageID # 6272) and that "the officers of MPD have demonstrated their dedication to protecting First Amendment rights regardless of protester opinion" (*id.* at PageID # 6243). Further, no fewer than five specific provisions of the consent decree forbid it.[9]

Yet the request appears to arise from a legitimate concern: that views on the various issues addressed during the focus groups may be skewed due to disproportionate participation by a vocal, but small, minority of Memphis residents. According to the City, certain City Council members and other local constituencies regularly raise concerns with the City that are at odds with those raised by the ACLU-TN and its supporters. To that end, the Monitoring Team has invited the City to propose additional constituencies and individuals that should be included in the focus groups, much as the ACLU-TN has encouraged its members and supporters to contact

---

[7] During the same call, the City mentioned that it has reached an agreement with the Tennessee Highway Patrol (THP) to access the speed cameras that THP has on the interstate due to the high number of shootings that happen there. The cameras are a live stream and do not record data. Our understanding is that MPD plans to purchase equipment that would allow officers to record the camera footage for review in case of an internet shooting. This scenario appears to implicate §§ G, H, and I of the *Kendrick* Consent Decree for many of the same reasons outlined in the August 21, 2019, Coordination Opinion.

[8] During the call, one member of the City's legal team stated, "They won't know who we are."

[9] *See, e.g.*, §§ C(1) ("[T]he City of Memphis shall not engage in political intelligence."); D (forbidding the City to "intercept, record, transcribe or otherwise interfere with any communication by means of electronic surveillance for the purpose of political intelligence"); E (forbidding the City to "infiltrate or pose as a member of any group or organization exercising First Amendment rights"); F(1) (forbidding the City to "disrupt, discredit, interfere with or otherwise harass any person exercising First Amendment rights"); and H(1) (forbidding the maintenance of personal information except when collected via and relevant to "a lawful investigation of criminal conduct").

the Monitoring Team.[10] The Monitoring Team wishes to include as broad a spectrum of Memphis residents as possible in its focus groups.

Anonymous, surreptitious observations of the focus groups by the very entity whose unlawful conduct necessitated the focus groups in the first place, however, is not the answer. That request is categorically denied.

B. July 29, 2019, RFA.

On July 29, 2019, the City explained that it will install Speed Cameras, whose purpose is student safety, near fifteen local schools. The cameras "will be activated 45 min before school starts and run a short period after school starts and 30 min before school ends and run a short period of time after school." (Email from B. McMullen to E. Stanton, attached as **Exhibit 3**.) "[D]ata that does not result in a ticket will be kept 90 days and the data resulting in a ticket will be kept 3 years. The data will be held by a third party (Conduent)." (*Ibid.*) The City will start installing the Speed Cameras in September 2019 and expects them to go live by December 2019. (*Ibid.*) The City has asked whether this proposed use of the cameras violates the consent decree.

This question implicates § H of the consent decree. Section H prohibits the City from "maintain[ing] personal information about any person unless it is collected in the course of a lawful investigation of criminal conduct." § H(1). It also prohibits the City from sharing "personal information . . . collected in the course of a lawful investigation of criminal conduct" unless the recipient is "another governmental law enforcement agency then engaged in a lawful investigation of criminal conduct." § H(2). As stated in the August 21, 2019, Coordination Opinion, I read this language to impose two applicable restrictions: (1) entirely against the sharing of personal information collected in any way other than via lawful criminal investigation (as such information may not be maintained in the first instance); and (2) against the sharing of personal information collected via lawful criminal investigation unless such sharing is with another governmental law enforcement agency and that agency already is engaged in a lawful criminal investigation.

Traffic offenses generally are classified as misdemeanors under Tennessee law. *See, e.g.*, Tenn. Code Ann. § 55-8-103 (classifying traffic offenses as misdemeanors unless "otherwise declared . . . with respect to particular offenses"). Thus, § H(1) appears to allow the City to collect personal information via the Speed Cameras as part of a "lawful investigation of criminal conduct." Where the data does not result in a ticket, however, that data "shall be destroyed," according to § H(1), rather than kept for ninety (90) days. Additionally, § H(2) appears to forbid the City from sharing the collected information with Conduent or any other non-law enforcement third party, as it prohibits the sharing of "personal information . . . collected in the course of a lawful investigation of criminal conduct" unless the recipient is "another governmental law enforcement agency then engaged in a lawful investigation of criminal conduct." Finally, the

---

[10] In fact, the ACLU-TN provided via email earlier today some resources to assist the Monitoring Team as it organizes focus groups and subsequent community forums.

Monitoring Team would like to know the law enforcement purpose for maintaining data that results in a ticket for three (3) years rather than a shorter amount of time.

C. August 5, 2019, RFA.

On August 5, 2019, a Shelby County Sherriff was involved in a fatal shooting near 201 Poplar. According to the City, the Sherriff's Office asked the MPD to control the scene, as the shooting occurred within City limits, and the TBI also was on the scene because the shooting involved a peace officer. At 3:46 P.M. that afternoon, the City requested through its legal counsel "permission for MPD to be able to go on social media to gauge the potential response to this situation and anticipate crowd swell." (Email from B. McMullen to E. Stanton, attached as **Exhibit 4**.) The City also noted "that there may be plans to have a larger gathering at another location, and [that] MPD wants to be able to be prepared in order to adequately provide public safety at that location." (*Ibid.*) Director Rallings elaborated in a follow-up email at 4:31 P.M., explaining "that the officers are terrified to use their personal accounts and [MPD] cannot force them to do so." (Email from M. Rallings to E. Stanton, attached as **Exhibit 5**.) According to Director Rallings, "[t]he prohibition on [alternate] social media account[s] is crippling MPD and may put our citizens['] safety at risk. We need to resolve asap before we have an El Paso type incident." (*Ibid.*)

I approved this request contemporaneously, conditioned on the City's maintaining a log of all social media search terms used in connection with this incident.[11] Please provide that search-term log as soon as possible and also include its contents in the City's next quarterly search-term report to the court.

D. August 22, 2019, RFA.

On August 22, 2019, after having reviewed the Monitoring Team's August 12, 2019, response to the City's letter of June 7, 2019, the City stated that it intended to raise with the court certain recommendations of the team regarding the City's security procedures for entering City

---

[11] I also responded separately to Director Rallings' email, stating the following:

> Director Rallings –
>
> Thank you for sharing this concern. Please tell your officers that they may use their personal devices and social media accounts but that any such use will be subject to the same auditing and reporting requirements that apply to official MPD devices and accounts. We recognize that MPD has a critical public safety function. The purpose of my team is not to interfere with or inhibit that function but to help guide it, consistent with the parameters that Judge McCalla has identified. As long as your officers report their social media use as we have requested, the Monitoring Team will be able to proceed according to the court's instructions.

(August 5, 2019, Email from E. Stanton to M. Rallings, attached as **Exhibit 6**.)

Hall. (*See* Email from B. McMullen to E. Stanton, attached as **Exhibit 7**.) In the interim, the City proposed a modified entry procedure:

> [U]ntil we can get some clarity from the Court (and I would like to bring it up Tuesday because this is so critical), we plan to advise the City Hall security team to first ask persons where they intend to go when they enter City Hall. If they advise that they are going to pay their taxes on the 3rd Floor or to attend City Council events open to the public, we will not require those individuals to show ID or sign in on the desk log. If individuals advise that they are visiting any other area, we will ask them to show ID and sign in on the desk log, and we will make a visitor's badge so that employees are aware that a non-employee is in the restricted area. The photo will be retained until after court on Tuesday.
>
> . . .
>
> Finally, with respect to 170 Main which houses MPD, parts of HR, Legal and the sex offender registry office, we will continue to require the visitors state their business and produce their identification, and we will produce a photo badge and maintain the information for security purposes.

(*Ibid.*) The City asked that I approve this interim approach until the City obtains "further clarification from the Court on Tuesday[, August 27, 2019]." (*Ibid.*)

I approved that request.

E. August 23, 2019, RFA.

Finally, this past Friday, August 23, 2019, the City made a request regarding its use of Crime Stoppers. (*See* Email from B. McMullen to E. Stanton, attached as **Exhibit 8**.) According to the City, when a crime is committed, the City encourages anyone with information related to the crime to call Crime Stoppers, which is "a standalone entity that is separate from MPD." (*Ibid.*) Crime Stoppers then shares that information that it receives with MPD. (*Ibid.*) The MPD has no way to determine how the caller obtained the information that it receives or whether the collection of the information complies with the consent decree. The City wants to know whether the MPD may continue to receive information from Crime Stoppers under the consent decree.

This request implicates § I of the consent decree. Section I forbids the City to "encourage, cooperate with, delegate, employ or contract with, or act at the behest of, any local, state, federal or private agency, or any person, to plan or conduct any . . . activity . . . prohibited by th[e] decree." As stated in the August 21, 2019, Coordination Opinion, I read this restriction to place the onus on the City to verify that any information it receives from governmental law enforcement agencies, non-law enforcement agencies, public and private entities, and individuals satisfies the same standards as information lawfully collected by the City itself.

Information collected by civilian residents of the City, shared with Crime Stoppers, and then shared with the MPD ordinarily would not implicate the First Amendment. The First Amendment restrains only the government, and not private individuals or organizations. Thus, the practices of private individuals and organizations do not offend the First Amendment even when those same practices, employed by the government, would violate it.

Section I of the consent decree, however, forbids the City to coordinate both with governmental entities—"any local, state, [or] federal" entity—and with any "private agency, or any person, to plan or conduct any . . . activity . . . prohibited by th[e] decree." As a result, the practices of private individuals or organizations may offend the consent decree if the City "encourage[s], cooperate[s] with, delegate[s], employ[s] or contract[s] with, or act[s] at the behest of" such private individuals or organizations "to plan or conduct any . . . activity . . . prohibited by th[e] decree." § I.

The only way to ensure that the City does not offend the consent decree in working with private individuals or organizations is to require the same verification process for information received from private individuals and organizations as I understand the consent decree to impose for receiving information from the FBI, the Secret Service, or any other law enforcement agencies. (*See generally* August 21, 2019, Coordination Opinion.) The City's ability to receive information from private citizens, either through Crime Stoppers or directly, is thus subject to verification that the information satisfies the same standards as information lawfully collected by the City itself.

III.
Conclusion.

All remaining questions about the City's prior RFAs and all outstanding RFAs by the City should now have been addressed. We look forward to seeing you tomorrow at the court's next hearing in this matter.

Sincerely,

BUTLER SNOW LLP

Edward L. Stanton III

ES:tw

cc: Bruce A. McMullen, Esq. (via email only)
Jim Letten, Esq. (via email only)
Gadson W. Perry, Esq. (via email only)

Exhibit 1

From: Silk, Jennie <jsilk@bakerdonelson.com>
Sent: Friday, July 12, 2019 4:41 PM
To: Edward L. Stanton III
Cc: Shanell Tyler; Will Perry; Glover, R. Mark; Tullis, Mary Wu; McMullen, Bruce; McMullen, Bruce
Subject: Search terms for Nathan Bedford Forrest Birthday Rally and Confirming Use of Cameras at Rally Tonight

Hi Ed,

As we discussed on the call today, a rally is planned this weekend to celebrate Nathan Bedford Forrest's birthday, which is tomorrow July 13. You instructed the City to send you the search terms that MPD needs to search on social media in order to adequately prepare for this event. Here is the list:

Confederate
NBF
Forrest
July 13
July 13, 1821
October 29
October 29, 1877
Statue
December 20, 2017
Sons of the Confederacy
SOC
Nathan Bedford Forrest
Friends of Nathan Bedford Forrest
Confederate901
Confederate 901
Taking Our Country Back
Hiwayman Operation Home Front
highwaymen
Rollin Memphis
KKK
Ku Klux Klan
Grand Wizard
Health Sciences Park
Lee Millar
Calvary General
Battle of Fort Pillow
Battle of Shiloh
Confederate Hero
Battle of Fort Donelson
Battle of Tupelo
KKK
Billy Roper
Shield Wall

Possible Counter protesters:
CCC
Coalition of Concerned Citizens
New Black Panthers
Antifa

Please understand that we are very sensitive to the issue of the counter-protester group names listed above, however, the City needs to prepare for the possibility of a large counter protest that could turn violent or become otherwise disruptive. As you know, whenever two ideologically opposite groups converge, things could erupt, similar to what happened in Charlottesville, Virginia.

This note also confirms that today the Monitoring team gave the City the greenlight to operate its SkyCops, Body Worn Cameras, and Dash Cams pursuant to the current MPD policy for each of those cameras at the rally planned for tonight centered on the release of journalist Manuel Duran from ICE custody.

Please let us know if you have any questions or concerns. Thank you and the team for taking the time to address these issues on the call today.

Best,

Jennie Vee Silk
Associate

Baker, Donelson, Bearman, Caldwell & Berkowitz, PC
2000 First Tennessee Building
165 Madison Avenue
Memphis, TN 38103

Phone 901.577.8212
Fax 901.577.0812
JSilk@bakerdonelson.com

Exhibit 2

From: McMullen, Bruce <Bruce.McMullen1@memphistn.gov>
Sent: Friday, July 19, 2019 4:28 PM
To: Edward L. Stanton III; Will Perry; Shanell Tyler; Jim Letten
Cc: Glover, R. Mark; Jill Silk; Saleem, Zayid-mem; Tullis, Mary Wu; Sink, Jennifer
Subject: Facebook inquery about Imposter
Attachments: SKM_C45819071914390.pdf; SKM_C45819071914391.pdf; SKM_C45819071914420.pdf

Ed, Will, Jim, & Shanell,

Attached is the letter from Facebook's Associate General Counsel, Andrea Kirkpatrick, and the subsequent emails discussing the imposter accounts in September 2019.

Before I get to those, in October 2016, I contacted Facebook about 5 imposter accounts that were created in the likeness of the Mayor, the Police Director, the City, and the Mayor's wife. See attached emails I exchanged with FBI Agent David Palmer, as well as my email to Facebook notifying them of the imposter accounts, requesting that they shut down the accounts, and advising them that I had reached out to the US Attorney's Office. Ultimately, we were unable to trace the origin of the Facebook accounts, although the FBI was able to trace 2 imposter Twitter accounts to Paul Garner.

Following the ACLU trial, MPD received a letter dated September 19, 2018 from Andrea Kirkpatrick. Initially, I thought the letter was fake but we verified it was in fact legitimate. I contacted Ms. Kirkpatrick by email on September 25, 2018 and inquired about the imposter accounts alleged to have been created by MPD. In an email of September 26th Ms. Kirkpatrick advised that Facebook took action on 6 accounts because they appeared to be "forensically related" to the "Bob Smith" account, but determined 3 were authentic and 3 were disabled for being fake. She provide us with the URLs of the three fake accounts but they were disabled.

We investigated but had no knowledge of any other imposter accounts other than "Bob Smith" which was deactivated. I did not know what "forensically related" meant, so I inquired with our Chief IS Officer Mike Rodriguez as to its meaning and whether he could determine the identity of the disabled Facebook accounts, including their creator (see email of Oct 3 2018 for his response). Mr. Rodriguez could not make any determinations. We also engaged an outside Cyber security attorney but he was also l unsuccessful.

Bruce McMullen
Chief Legal Officer/City Attorney
125 N. Main, Room 336
Memphis, Tennessee 38103
(901) 576-6614 – Office
(901) 576-6531 – Fax
bruce.mcmullen1@memphistn.gov

McMullen, Bruce

From: Palmer, David E. (ME) (FBI) <David.Palmer2@ic.fbi.gov>
Sent: Friday, October 28, 2016 2:11 PM
To: McMullen, Bruce
Subject: RE: IMMINENT MATTER--imposter account of Public official

David E. Palmer
Special Agent
FBI Memphis Division
225 N. Humphreys Blvd.
Memphis, TN 38120
Office: 901-747-9607
Cell: 901-233-3213
david.palmer2@ic.fbi.gov

From: McMullen, Bruce [mailto:Bruce.McMullen1@memphistn.gov]
Sent: Friday, October 28, 2016 2:09 PM
To: Palmer, David E. (ME) (FBI)
Subject: Fwd: IMMINENT MATTER--imposter account of Public official

Sent from my iPhone

Begin forwarded message:

> **From:** "McMullen, Bruce" <Bruce.McMullen1@memphistn.gov>
> **Date:** October 28, 2016 at 12:32:10 PM CDT
> **To:** "records@facebook.com" <records@facebook.com>
> **Cc:** "Sink, Jennifer" <Jennifer.Sink@memphistn.gov>
> **Subject: IMMINENT MATTER--imposter account of Public official**
>
> Dear Facebook legal
>
> I am the Chief Legal officer for the City of Memphis Tennessee. Someone has created at least 5 imposter accounts all of which claim to be the Mayor of Memphis' page or His wife's page.
>
> http://cp.mcafee.com/d/k-Kr6zqb0UsUYyqehPNISyyyyM-C-UOrhhhhovjshhdCPpJnRlysGjxN6FASCCWOaIXp0lZTni7Lm5nJjp5mdto5thd7bUGCg7e47n1SKc8CPpISr9PCJhbcasXJL8lGlVv49hCmEuTdMtx9SfKDjErdELef6PtPqpJUTsTsSyrh

http://cp.mcafee.com/d/FZsScy0Qrho73D7AjhOeudCQkkkm7QTT6jqaaab3Wrya9ISrdG-GIjBise8RcCQQTmhlDr82LKWWgZWMGZGr8GNHH0HG9EVv5kO0VMwWUeRNx4SrdCPpesRG9pxjDtJV2JiLbU7q2_Q_Wj6Zblzx9SfKDjErdELef6PtPqpJUTsTsSyrh
http://cp.mcafee.com/d/2DRPoQ73gwcCQm1MVNV4QszDzpJ5555xZdZNASyyyyM-CUyyrdCPqLGH4VkD3ydj9JddRAlpSO0HXKKAfuIaLqCOaIqWMaWyqenNlcwes8eK3JsohdCPpISjDdqymokVTrugHkHO-3vGH4VkU03x9SfKDjErdELef6PtPqpJUTsTsSyrh
http://cp.mcafee.com/d/2DRPow82gQcCQm1MVNV4QszDzpJ5555xZdZNASyyyyM-CUyyrdCPqLGH4VkD3ydj9JddRAlpSO0HXKKAfuIaLqCOaIqWMaWyqenNlcwes8eK3JsohdCPpISjDdqymokVTrugHkHO-6zCWcSUMCSJx9SfKDjErdELef6PtPqpJUTsTsSyrh
http://cp.mcafee.com/d/FZsSd39J5wsesuhd78VUSrhhhhovjvspdEEEEIfFK8ECPpISHWGNel9MUzkOrjjtp5mtlwa-XHF3TH2HSFlyH6KI2KECzBYlj83D23HwXn64jpISrdAVPmEBC5etSTAaRaYLyLGH4VkSzIpmaUrdELef6PtPqpJUTsTsSyrh

The comments on the different sites are not only vulgar and inappropriate, the sites themselves are misleading and poses a threat to public safety. Consequently, we would like your assistance in shutting these sites down. We have contacted the US Attorney for the Western District of Tennessee and notified him of the problem. He has notified the FBI and we are expecting to hear from them. In the interim, would you please shut these sites down as I understand it is Facebook's policy not to support imposter accounts.

Bruce McMullen
Chief Legal Officer/City Attorney
125 N. Main, Room 336
Memphis, Tennessee 38103
(901) 576-6614 – Office
(901) 576-6531 – Fax
bruce.mcmullen1@memphistn.gov

McMullen, Bruce

From: Palmer, David E. (ME) (FBI) <David.Palmer2@ic.fbi.gov>
Sent: Monday, October 31, 2016 9:31 AM
To: McMullen, Bruce
Subject: RE: IMMINENT MATTER--imposter account of Public official

Mr. McMullen,

It appears that most of the Facebook sites listed below have been shut down with the exception of "memphisasfrick". Do you know if anyone took screen shots or preserved any of the content from these sites prior the them being closed?

Thanks,

David E. Palmer
Special Agent
FBI Memphis Division
225 N. Humphreys Blvd.
Memphis, TN 38120
O: 901-747-9607
C: 901-233-3213
david.palmer2@ic.fbi.gov

From: McMullen, Bruce [mailto:Bruce.McMullen1@memphistn.gov]
Sent: Friday, October 28, 2016 2:09 PM
To: Palmer, David E. (ME) (FBI)
Subject: Fwd: IMMINENT MATTER--imposter account of Public official

Sent from my iPhone

Begin forwarded message:

> **From:** "McMullen, Bruce" <Bruce.McMullen1@memphistn.gov>
> **Date:** October 28, 2016 at 12:32:10 PM CDT
> **To:** "records@facebook.com" <records@facebook.com>
> **Cc:** "Sink, Jennifer" <Jennifer.Sink@memphistn.gov>
> **Subject: IMMINENT MATTER--imposter account of Public official**
>
> Dear Facebook legal
>
> I am the Chief Legal officer for the City of Memphis Tennessee. Someone has created at least 5 imposter accounts all of which claim to be the Mayor of Memphis' page or His wife's page.

http://cp.mcafee.com/d/avndy0s81NJ5wsed7ar35T3pJ5555xZdZNASyyyyM-CUyyrdCPqLGH4VkD3ydj9JfXCzAlod7a10lh7fKemIYaLLcS5m44S1kwYUUaA1TCzCP6K6zDXfCPpISr9PCJhbcasXJL8lGlVv49hCmEuTdMtx9SfKDjErdELef6PtPqpJUTsTsSyrh
http://cp.mcafee.com/d/1jWVIedEI3xNEVjooKUrdEEEEIfFLKcCQkkkm7QT4kjpISrlZloDaAUshGpdF_sQsyH1EVg82G8VZNORDxlZVCMGMwCMaA7D71kweYQsSoRMQs_pYSrdCPpesRG9pxjDtJV2JiLbU7q2_Q_Wj6ZblZx9SfKDjErdELef6PtPqpJUTsTsSyrh
http://cp.mcafee.com/d/1jWVIp418p4zqb0UsqekS6bK6Pqaaab3WrXz9J5555xZdN54SrdCRvlm9OFe74qCjqvTd78GMqek20GyevssJpUlvupIaI89I2F1VNMl83Ld7dCdsd7fSvdCPpISjDdqymokVTrugHkHO-3vGH4VkU03x9SfKDjErdELef6PtPqpJUTsTsSyrh
http://cp.mcafee.com/d/5fHCMUp43qb0UsqekS6bK6Pqaaab3WrXz9J5555xZdN54SrdCRvlm9OFe74qCjqvTd78GMqek20GyevssJpUlvupIaI89I2F1VNMl83Ld7dCdsd7fSvdCPpISjDdqymokVTrugHkHO-6zCWcSUMCSJx9SfKDjErdELef6PtPqpJUTsTsSyrh
http://cp.mcafee.com/d/k-Kr40Uq41ASyMe76zBdxyXxISyyyyM-C-UOrhhhhovjshhdCPpJnRlysGjxN6FASDZPhOaI6zB0waEzDT7bmu5nTCr2H22r0Gguss5i0XPhPpzn3hPZDPpISrdAVPmEBC5etSTAaRaYLyLGH4VkSzIpmaUrdELef6PtPqpJUTsTsSyrh

The comments on the different sites are not only vulgar and inappropriate, the sites themselves are misleading and poses a threat to public safety. Consequently, we would like your assistance in shutting these sites down. We have contacted the US Attorney for the Western District of Tennessee and notified him of the problem. He has notified the FBI and we are expecting to hear from them. In the interim, would you please shut these sites down as I understand it is Facebook's policy not to support imposter accounts.

Bruce McMullen
Chief Legal Officer/City Attorney
125 N. Main, Room 336
Memphis, Tennessee 38103
(901) 576-6614 – Office
(901) 576-6531 – Fax
bruce.mcmullen1@memphistn.gov

September 19, 2018

By Email and via FedEx

Mr. Michael Rallings
Director, Memphis Police Department
Memphis Police Department
170 N. Main Street
Memphis, TN 38103

Dear Mr. Rallings:

We recently learned through media reports and the Electronic Frontier Foundation (EFF) that the Memphis Police Department created fake Facebook accounts and impersonated legitimate Facebook users as part of its investigation of alleged criminal conduct unrelated to Facebook. We write to underscore that this activity violates our terms of service. The Police Department should cease all activities on Facebook that involve the use of fake accounts or impersonation of others.

People come to Facebook to connect and share with real people using their authentic identities. This core principle is what differentiates Facebook from other services on the Internet. Our authenticity policies are intended to create a safe environment where people can trust and hold one another accountable. Operating fake accounts violates the terms and policies that govern the Facebook service, and undermines trust in our community (https://www.facebook.com/communitystandards/misrepresentation).

Anyone who creates a Facebook account agrees to abide by our Community Standards, which expressly prohibit the creation and use of fake accounts. The Community Standards provide as follows:

- Do not misrepresent your identity by using a name that does not abide by our name policies (https://www.facebook.com/help/112146705538576) or providing a false date of birth.
- Do not misuse our profiles product by:
  - Creating a profile for someone under thirteen years old
  - Maintaining multiple accounts
  - Creating inauthentic profiles
  - Sharing an account with any other person
  - Creating another account after being banned from the site
  - Evading the registration requirements outlined in our Terms of Service (https://www.facebook.com/legal/terms)
- Do not impersonate others by:
  - Using their images with the explicit aim to deceive people
  - Creating a profile assuming the persona of or speaking for another person or entity

- Creating a Page assuming to be or speak for another person or entity for whom the user is not authorized to do so.

- Do not engage in authentic behavior, which includes creating, managing, or otherwise perpetuating:
  - Accounts that are fake
  - Accounts that have fake names
  - Accounts that participate in, or claim to engage in, coordinated inauthentic behavior, meaning that multiple accounts are working together to do any of the following:
    - Mislead people about the origin of content
    - Mislead people about the destination of links off our services (for example, providing a display URL that does not match the destination URL)
    - Mislead people in an attempt to encourage shares, likes, or clicks
    - Mislead people to conceal or enable the violation of other policies under the Community Standards

Facebook has made clear that law enforcement authorities are subject to these policies. We regard this activity as a breach of Facebook's terms and policies, and as such we have disabled the fake accounts that we identified in our investigation.

We request that the Police Department, its members, and any others acting on its behalf cease all activities on Facebook that involve impersonation or that otherwise violate our policies.

Please contact us if you have any questions or concerns.

Sincerely,

Andrea Kirkpatrick
Director and Associate General Counsel, Security

earthsmart
FedEx carbon-neutral
envelope shipping

Align top of FedEx Express® shipping label here

ORIGIN ID:PAOA (650) 739-9596
KURTIS HUBBELL
FACEBOOK
1 HACKER WAY

MENLO PARK, CA 94025
UNITED STATES US

SHIP DATE: 19SEP18
ACTWGT: 1.00 LB MAN
CAD: 0589497/CAFE3210

BILL SENDER

TO MR. MICHAEL RALLINGS
MEPHIS POLICE DEPARTMENT
170 N MAIN STREET

MEMPHIS TN 38103
(901) 636-3700
REF: ANDREA KIRPATRICK

FedEx Express

TRK# 0201 4437 9255 9499

THU - 20 SEP 10:30A
PRIORITY OVERNIGHT

XH NQAA

38103
TN-US MEM

Part # 156148-434 RIT EXP 04/19

RT589 1 10:30 A 9499 09.20 FZ

McMullen, Bruce

From: Andrea Kirkpatrick <andreak@fb.com>
Sent: Wednesday, September 26, 2018 1:51 PM
To: McMullen, Bruce; Jay Nancarrow
Cc: 'Joy, Justin N.'; Sink, Jennifer
Subject: Re: Letter from Andrea Kirkpatrick

Follow Up Flag: Follow up
Flag Status: Flagged

Dear Mr. McMullen:

Thank you for reaching out and for looking into this matter more closely on behalf of the City of Memphis.

We took action on six additional accounts because they appeared to be inauthentic and were forensically related to the "Bob Smith" account that was the subject of The Appeal's August 2, 2018 article (https://theappeal.org/memphis-police-surveillance-black-lives-matter-facebook-profile-exclusive/).

Of the six accounts, three were checkpointed and three were disabled for being fake. The account holders of the three checkpointed accounts have since submitted the information necessary to authenticate the accounts. As a result, those accounts have been reactivated.

The accounts that were disabled as fake remain disabled. The URLs associated with those accounts are:

- URL: https://www.facebook.com/100009045433820
- URL: http://facebook.com/100020798830432
- URL: https://www.facebook.com/100025331090444

Should you require additional information from Facebook about these accounts, please refer to our Law Enforcement Guidelines (https://www.facebook.com/safety/groups/law/guidelines/) which serve as our operational guidelines for law enforcement official seeking records from Facebook.

Best,

Andrea Kirkpatrick | facebook | Director & Associate General Counsel, Security |
1 Hacker Way, Menlo Park, CA 94025

From: "McMullen, Bruce" <Bruce.McMullen1@memphistn.gov>
Date: Tuesday, 25 September 2018 8:07 AM
To: Jay Nancarrow <jcn@fb.com>

Cc: "'Joy, Justin N.'" <JJoy@LewisThomason.com>, "Sink, Jennifer" <Jennifer.Sink@memphistn.gov>, Andrea Kirkpatrick <andreak@fb.com>
Subject: RE: Letter from Andrea Kirkpatrick

Ms. Kirkpatrick,

I am the Chief Legal Officer for the City of Memphis. Under my jurisdiction are the divisions of the City, including Memphis Police Department (MPD). I appreciate your letter dated September 20th and will address it further in a future correspondence. However, in his email Mr. Nancarrow indicated there were 6 "related accounts." Consequently, I am investigating the creation and use of 6 "related accounts" allegedly linked to MPD.

Unfortunately, I am not sure what "related accounts" means in this context. Are they MPD accounts, MPD employee accounts, family members accounts etc.. Could you please define and clarify?

Additionally, if there is a concern that they are MPD sanctioned or MPD controlled accounts or that they are used in MPD's business, please provide me with as much information as possible so that I can investigate and take appropriate action. Please include the name, when it was created, and any information traced back to the creator.

Bruce McMullen
Chief Legal Officer/City Attorney
125 N. Main, Room 336
Memphis, Tennessee 38103
(901) 576-6614 – Office
(901) 576-6531 – Fax
bruce.mcmullen1@memphistn.gov

From: Jay Nancarrow [mailto:jcn@fb.com]
Sent: Monday, September 24, 2018 7:32 PM
To: McMullen, Bruce
Cc: 'Joy, Justin N.'; Sink, Jennifer; Andrea Kirkpatrick
Subject: Re: Letter from Andrea Kirkpatrick

Dear Mr. McMullen,

I can confirm that the letter you received from Andrea Kirkpatrick is legitimate. I'm copying her on this response for further validation. Upon receiving the initial report of the fake account that was in use, we disabled it and then looked for related accounts. As a result, we ended up taking action on an additional six accounts. Regarding your remaining questions about providing additional information concerning these accounts, I believe Andrea is best placed to respond.

Thank you,

Jay Nancarrow

From: "McMullen, Bruce" <Bruce.McMullen1@memphistn.gov>
Date: Monday, September 24, 2018 at 2:41 PM
To: Jay Nancarrow <jcn@fb.com>
Cc: "'Joy, Justin N.'" <JJoy@LewisThomason.com>, "Sink, Jennifer" <Jennifer.Sink@memphistn.gov>
Subject: Letter from Andrea Kirkpatrick

Dear Mr. Nancarrow,

I am the Chief Legal Officer for the City of Memphis. As such, I represent Memphis Police Department. I am trying to authenticate a letter the Memphis Police Department received from Andrea Kirkpatrick dated September 20, 2018. Attached is a copy of the letter. Also, I understand from unconfirmed press reports that Facebook found 6 additional accounts associated with MPD's account. If this is accurate, please provide me with information about those related accounts including names used, dates originated, and last postings, and what action was taken by Facebook on these accounts.

Bruce McMullen
Chief Legal Officer/City Attorney
125 N. Main, Room 336
Memphis, Tennessee 38103
(901) 576-6614 – Office
(901) 576-6531 – Fax
bruce.mcmullen1@memphistn.gov

McMullen, Bruce

From: Rodriguez, Mike
Sent: Wednesday, October 03, 2018 5:36 PM
To: McMullen, Bruce
Cc: 'Joy, Justin N.'; Sink, Jennifer
Subject: RE: Confidential attorney client information

Bruce,

"forensically related" would mean that when Facebook looked at the Facebook pages they found similar data associated with each of the urls in question. Meaning – perhaps the same computer was used to create the account, the same user id was used to create the account – or something like that. A MAC address or IP address across the urls were related. Since the account have been deactivated by Facebook we do not have any ability to do any forensics analysis.

I will have the IS team take a look in the proxy logs and see if we can identify a city employee that might have accessed the pages in question.

Regards,
Mike

From: McMullen, Bruce
Sent: Wednesday, October 3, 2018 2:34 PM
To: Rodriguez, Mike <Mike.Rodriguez@memphistn.gov>
Cc: 'Joy, Justin N.' <JJoy@LewisThomason.com>; Sink, Jennifer <Jennifer.Sink@memphistn.gov>
Subject: Confidential attorney client information

Mike,

Look at the three URLs that Facebook says are disconnected. Is there any information we can get on those disconnected URLs? I am trying to see who they are and figure out how they are linked them to MPD. Also, can you tell me specifically what "forensically related" means?

From: Andrea Kirkpatrick [mailto:andreak@fb.com]
Sent: Wednesday, September 26, 2018 1:51 PM
To: McMullen, Bruce; Jay Nancarrow
Cc: 'Joy, Justin N.'; Sink, Jennifer
Subject: Re: Letter from Andrea Kirkpatrick

Dear Mr. McMullen:

Thank you for reaching out and for looking into this matter more closely on behalf of the City of Memphis.

We took action on six additional accounts because they appeared to be inauthentic and were forensically related to the "Bob Smith" account that was the subject of The Appeal's August 2, 2018 article (https://theappeal.org/memphis-police-surveillance-black-lives-matter-facebook-profile-exclusive/).

Of the six accounts, three were checkpointed and three were disabled for being fake. The account holders of the three checkpointed accounts have since submitted the information necessary to authenticate the accounts. As a result, those accounts have been reactivated.

The accounts that were disabled as fake remain disabled. The URLs associated with those accounts are:

- URL: https://www.facebook.com/100009045433820
- URL: http://facebook.com/100020798830432
- URL: https://www.facebook.com/100025331090444

Should you require additional information from Facebook about these accounts, please refer to our Law Enforcement Guidelines (https://www.facebook.com/safety/groups/law/guidelines/) which serve as our operational guidelines for law enforcement official seeking records from Facebook.

Best,

Andrea Kirkpatrick | facebook | Director & Associate General Counsel, Security |
1 Hacker Way, Menlo Park, CA 94025

From: "McMullen, Bruce" <Bruce.McMullen1@memphistn.gov>
Date: Tuesday, 25 September 2018 8:07 AM
To: Jay Nancarrow <jcn@fb.com>
Cc: "'Joy, Justin N.'" <JJoy@LewisThomason.com>, "Sink, Jennifer" <Jennifer.Sink@memphistn.gov>, Andrea Kirkpatrick <andreak@fb.com>
Subject: RE: Letter from Andrea Kirkpatrick

Ms. Kirkpatrick,

I am the Chief Legal Officer for the City of Memphis. Under my jurisdiction are the divisions of the City, including Memphis Police Department (MPD). I appreciate your letter dated September 20th and will address it further in a future correspondence. However, in his email Mr. Nancarrow indicated there were 6 "related accounts." Consequently, I am investigating the creation and use of 6 "related accounts" allegedly linked to MPD.

Unfortunately, I am not sure what "related accounts" means in this context. Are they MPD accounts, MPD employee accounts, family members accounts etc.. Could you please define and clarify?

Additionally, if there is a concern that they are MPD sanctioned or MPD controlled accounts or that they are used in MPD's business, please provide me with as much information as possible so that I can investigate and take appropriate action. Please include the name, when it was created, and any information traced back to the creator.

Bruce McMullen
Chief Legal Officer/City Attorney
125 N. Main, Room 336
Memphis, Tennessee 38103

(901) 576-6614 – Office
(901) 576-6531 – Fax
bruce.mcmullen1@memphistn.gov

From: Jay Nancarrow [mailto:jcn@fb.com]
Sent: Monday, September 24, 2018 7:32 PM
To: McMullen, Bruce
Cc: 'Joy, Justin N.'; Sink, Jennifer; Andrea Kirkpatrick
Subject: Re: Letter from Andrea Kirkpatrick

Dear Mr. McMullen,

I can confirm that the letter you received from Andrea Kirkpatrick is legitimate. I'm copying her on this response for further validation. Upon receiving the initial report of the fake account that was in use, we disabled it and then looked for related accounts. As a result, we ended up taking action on an additional six accounts. Regarding your remaining questions about providing additional information concerning these accounts, I believe Andrea is best placed to respond.

Thank you,

Jay Nancarrow

From: "McMullen, Bruce" <Bruce.McMullen1@memphistn.gov>
Date: Monday, September 24, 2018 at 2:41 PM
To: Jay Nancarrow <jcn@fb.com>
Cc: "'Joy, Justin N.'" <JJoy@LewisThomason.com>, "Sink, Jennifer" <Jennifer.Sink@memphistn.gov>
Subject: Letter from Andrea Kirkpatrick

Dear Mr. Nancarrow,

I am the Chief Legal Officer for the City of Memphis. As such, I represent Memphis Police Department. I am trying to authenticate a letter the Memphis Police Department received from Andrea Kirkpatrick dated September 20, 2018. Attached is a copy of the letter. Also, I understand from unconfirmed press reports that Facebook found 6 additional accounts associated with MPD's account. If this is accurate, please provide me with information about those related accounts including names used, dates originated, and last postings, and what action was taken by Facebook on these accounts.

Bruce McMullen
Chief Legal Officer/City Attorney
125 N. Main, Room 336
Memphis, Tennessee 38103
(901) 576-6614 – Office
(901) 576-6531 – Fax
bruce.mcmullen1@memphistn.gov

Exhibit 3

From: McMullen, Bruce <Bruce.McMullen1@memphistn.gov>
Sent: Monday, July 29, 2019 9:16 AM
To: Edward L. Stanton III; Will Perry; Jim Letten; Shanell Tyler
Cc: Glover, R. Mark; Jill Silk; Tullis, Mary Wu; Sink, Jennifer
Subject: Blanchard v The City - Monitor communication

Ed, Jim, Will & Shanell,

The City is installing speed Camera in 15 locations (attached is the location map). The Cameras are similar to red light cameras that are currently in use. The purpose of the cameras is for student safety. They will be located near 15 schools to control traffic during early morning hours and after school. They will be activated 45 min before school starts and run a short period after school starts and 30 min before school ends and run a short period of time after school.

The data that does not result in a ticket will be kept 90 days and the data resulting in a ticket will be kept 3 years. The data will be held by a third party (Conduent). We will began installation in September and should have all systems live by December 2019.

Please advise whether the usage of these cameras as described above violates the consent decree?

Exhibit 4

From: McMullen, Bruce <Bruce.McMullen1@memphistn.gov>
Sent: Monday, August 05, 2019 2:46 PM
To: Edward L. Stanton III; Will Perry
Cc: Rallings, Director Michael; Saleem, Zayid-mem; Glover, R. Mark; Jill Silk; Tullis, Mary Wu; Sink, Jennifer; Fletcher, Michael; Crowe, Deputy Chief Don
Subject: Exigent circunstance request to Monitor

Importance: High

Ed,

Earlier today, a Shelby County Sheriff was involved in a fatal shooting near 201 Poplar. Almost immediately, a crowd gathered. MPD was asked by the Sheriff's Office to control the scene (the incident within MPD's jurisdiction in that it was in the City). TBI is on the scene, since it is an officer-involved shooting.

MPD is providing crowd control for public safety and has taken measures such as using bike racks to set up a perimeter. We are requesting permission for MPD to be able to go on social media to gauge the potential response to this situation and anticipate crowd swell. Also a concern is that there may be plans to have a larger gathering at another location, and MPD wants to be able to be prepared in order to adequately provide public safety at that location.

Per our conversation just a few moments ago, you have authorized this request, conditioned upon keeping a log of the search terms used.

Bruce McMullen
Chief Legal Officer/City Attorney
125 N. Main, Room 336
Memphis, Tennessee 38103
(901) 576-6614 – Office
(901) 576-6531 – Fax
bruce.mcmullen1@memphistn.gov

Exhibit 5

From: Rallings, Director Michael <Michael.Rallings@memphistn.gov>
Sent: Monday, August 05, 2019 3:31 PM
To: Edward L. Stanton III; McMullen, Bruce; Will Perry
Cc: Saleem, Zayid-mem; Glover, R. Mark; Jill Silk; Tullis, Mary Wu; Sink, Jennifer; Fletcher, Michael; Crowe, Deputy Chief Don
Subject: Re: Exigent circumstance request to Monitor

The problem is that the officers are terrified to use their personal accounts and we can not force them to do so.

The prohibition on a akternate social media account is crippling MPD and may put our citizens safety at risk. We need to resolve asap before we have an El Paso type incident.

Director Michael W. Rallings

Memphis Police Department

170 N. Main, Suite 12-01

Memphis, TN 38103

Phone (901) 636-3700

Fax (901 636-3502

Community Outreach Program (C.O.P), a proactive initiative developed by the Memphis PoliceDepartment, to improve the quality of life of citizens and reduce juvenile violence, utilizing crime prevention techniques through identification, enforcement and education within the community.

From: Edward L. Stanton III
Sent: Monday, August 5, 2019 2:54:06 PM
To: McMullen, Bruce ; Will Perry
Cc: Rallings, Director Michael ; Saleem, Zayid-mem ; Glover, R. Mark ; Jill Silk ; Tullis, Mary Wu ; Sink, Jennifer ; Fletcher, Michael ; Crowe, Deputy Chief Don
Subject: RE: Exigent circumstance request to Monitor

Bruce –

Confirmed.

ELS

Edward L. Stanton III
Butler Snow LLP

D: (901) 680-7369 | F: (901) 680-7201
6075 Poplar Avenue, Suite 500, Memphis, TN 38119
P.O. Box 171443, Memphis, TN 38187-1443
Edward.Stanton@butlersnow.com | vCard | Bio

Twitter | LinkedIn | Facebook | YouTube

From: McMullen, Bruce [mailto:Bruce.McMullen1@memphistn.gov]
Sent: Monday, August 05, 2019 2:46 PM
To: Edward L. Stanton III; Will Perry
Cc: Rallings, Director Michael; Saleem, Zayid-mem; Glover, R. Mark; Jill Silk; Tullis, Mary Wu; Sink, Jennifer; Fletcher, Michael; Crowe, Deputy Chief Don
Subject: Exigent circunstance request to Monitor
Importance: High

Ed,

Earlier today, a Shelby County Sheriff was involved in a fatal shooting near 201 Poplar. Almost immediately, a crowd gathered. MPD was asked by the Sheriff's Office to control the scene (the incident within MPD's jurisdiction in that it was in the City). TBI is on the scene, since it is an officer-involved shooting.

MPD is providing crowd control for public safety and has taken measures such as using bike racks to set up a perimeter. We are requesting permission for MPD to be able to go on social media to gauge the potential response to this situation and anticipate crowd swell. Also a concern is that there may be plans to have a larger gathering at another location, and MPD wants to be able to be prepared in order to adequately provide public safety at that location.

Per our conversation just a few moments ago, you have authorized this request, conditioned upon keeping a log of the search terms used.

Bruce McMullen
Chief Legal Officer/City Attorney
125 N. Main, Room 336
Memphis, Tennessee 38103

(901) 576-6614 – Office
(901) 576-6531 – Fax
bruce.mcmullen1@memphistn.gov

Exhibit 6

From: Edward L. Stanton III
Sent: Monday, August 05, 2019 4:07 PM
To: 'Rallings, Director Michael'; McMullen, Bruce; Will Perry
Cc: Saleem, Zayid-mem; Glover, R. Mark; Jill Silk; Tullis, Mary Wu; Sink, Jennifer; Fletcher, Michael; Crowe, Deputy Chief Don
Subject: RE: Exigent circumstance request to Monitor

Director Rallings –

Thank you for sharing this concern. Please tell your officers that they may use their personal devices and social media accounts but that any such use will be subject to the same auditing and reporting requirements that apply to official MPD devices and accounts. We recognize that MPD has a critical public safety function. The purpose of my team is not to interfere with or inhibit that function but to help guide it, consistent with the parameters that Judge McCalla has identified. As long as your officers report their social media use as we have requested, the Monitoring Team will be able to proceed according to the court's instructions.

Best,

ELS

Edward L. Stanton III
Butler Snow LLP

D: (901) 680-7369 | F: (901) 680-7201
6075 Poplar Avenue, Suite 500, Memphis, TN 38119
P.O. Box 171443, Memphis, TN 38187-1443
Edward.Stanton@butlersnow.com | vCard | Bio

Twitter | LinkedIn | Facebook | YouTube

From: Rallings, Director Michael [mailto:Michael.Rallings@memphistn.gov]
Sent: Monday, August 05, 2019 3:31 PM
To: Edward L. Stanton III; McMullen, Bruce; Will Perry
Cc: Saleem, Zayid-mem; Glover, R. Mark; Jill Silk; Tullis, Mary Wu; Sink, Jennifer; Fletcher, Michael; Crowe, Deputy Chief Don
Subject: Re: Exigent circumstance request to Monitor

The problem is that the officers are terrified to use their personal accounts and we can not force them to do so.

The prohibition on a akternate social media account is crippling MPD and may put our citizens safety at risk. We need to resolve asap before we have an El Paso type incident.

Director Michael W. Rallings

Memphis Police Department

170 N. Main, Suite 12-01

Memphis, TN 38103

Phone (901) 636-3700

Fax (901 636-3502

Community Outreach Program (C.O.P), a proactive initiative developed by the Memphis PoliceDepartment, to improve the quality of life of citizens and reduce juvenile violence, utilizing crime prevention techniques through identification, enforcement and education within the community.

From: Edward L. Stanton III
Sent: Monday, August 5, 2019 2:54:06 PM
To: McMullen, Bruce ; Will Perry
Cc: Rallings, Director Michael ; Saleem, Zayid-mem ; Glover, R. Mark ; Jill Silk ; Tullis, Mary Wu ; Sink, Jennifer ; Fletcher, Michael ; Crowe, Deputy Chief Don
Subject: RE: Exigent circumstance request to Monitor

Bruce –

Confirmed.

ELS

Edward L. Stanton III
Butler Snow LLP

D: (901) 680-7369 | F: (901) 680-7201
6075 Poplar Avenue, Suite 500, Memphis, TN 38119
P.O. Box 171443, Memphis, TN 38187-1443
Edward.Stanton@butlersnow.com | vCard | Bio

Twitter | LinkedIn | Facebook | YouTube

From: McMullen, Bruce [mailto:Bruce.McMullen1@memphistn.gov]
Sent: Monday, August 05, 2019 2:46 PM
To: Edward L. Stanton III; Will Perry
Cc: Rallings, Director Michael; Saleem, Zayid-mem; Glover, R. Mark; Jill Silk; Tullis, Mary Wu; Sink, Jennifer; Fletcher, Michael; Crowe, Deputy Chief Don
Subject: Exigent circumstance request to Monitor
Importance: High

Ed,

Earlier today, a Shelby County Sheriff was involved in a fatal shooting near 201 Poplar. Almost immediately, a crowd gathered. MPD was asked by the Sheriff's Office to control the scene (the incident within MPD's jurisdiction in that it was in the City). TBI is on the scene, since it is an officer-involved shooting.

MPD is providing crowd control for public safety and has taken measures such as using bike racks to set up a perimeter. We are requesting permission for MPD to be able to go on social media to gauge the potential response to this situation and anticipate crowd swell. Also a concern is that there may be plans to have a larger gathering at another location, and MPD wants to be able to be prepared in order to adequately provide public safety at that location.

Per our conversation just a few moments ago, you have authorized this request, conditioned upon keeping a log of the search terms used.

Bruce McMullen
Chief Legal Officer/City Attorney
125 N. Main, Room 336
Memphis, Tennessee 38103
(901) 576-6614 – Office
(901) 576-6531 – Fax
bruce.mcmullen1@memphistn.gov

Exhibit 7

From: McMullen, Bruce <Bruce.McMullen1@memphistn.gov>
Sent: Thursday, August 22, 2019 2:15 PM
To: Edward L. Stanton III; Will Perry; Shanell Tyler; Jim Letten
Cc: Glover, R. Mark; Jill Silk; Tullis, Mary Wu; Sink, Jennifer
Subject: Approval requested

Importance: High

Ed,

We are continuing to review your letter of August 12, 2019. I wanted to email you immediately to discuss clarification of your response to our Scenario #10 regarding security procedures for entering City Hall. Because your response would result in a massive operational change, and change in how we assess threats to employees (i.e., disgruntled former employees or someone under a restraining order), we wanted to make sure we were 100% clear on the directions for new security procedures or approach for persons entering City Hall and that you and the Court deem permissible under the Consent Decree.

Consequently, until we can get some clarity from the Court (and I would like to bring it up Tuesday because this is so critical), we plan to advise the City Hall security team to first ask persons where they intend to go when they enter City Hall. If they advise that they are going to pay their taxes on the 3rd Floor or to attend City Council events open to the public, we will not require those individuals to show ID or sign in on the desk log. If individuals advise that they are visiting any other area, we will ask them to show ID and sign in on the desk log, and we will make a visitor's badge so that employees are aware that a non-employee is in the restricted area. The photo will be retained until after court on Tuesday. Please confirm if that is acceptable until we can get further clarification from the Court on Tuesday.

Finally, with respect to 170 Main which houses MPD, parts of HR, Legal and the sex offender registry office, we will continue to require the visitors state their business and produce their identification, and we will produce a photo badge and maintain the information for security purposes.

Bruce McMullen
Chief Legal Officer/City Attorney
125 N. Main, Room 336
Memphis, Tennessee 38103
(901) 576-6614 – Office
(901) 576-6531 – Fax
bruce.mcmullen1@memphistn.gov

Exhibit 8

From: McMullen, Bruce <Bruce.McMullen1@memphistn.gov>
Sent: Friday, August 23, 2019 3:42 PM
To: Edward L. Stanton III; Will Perry; Shanell Tyler
Cc: mglover@bakerdonelson.com; Jill Silk; mtullis@bakerdonelson.com; Sink, Jennifer; Saleem, Zayid-mem
Subject: Request for Approval

Ed,

As you are aware, MPD uses an information/evidence gathering entity called "Crime Stoppers." When a crime is committed, there is usually a marketing campaign for anyone with any information to call a number and provide that information. The caller can remain anonymous or give personal information for follow up so that they can collect the cash reward. Crime Stoppers is a standalone entity that is separate from MPD; however, the information is transmitted to MPD.

MPD has no way of verifying how the caller got his/her intel and certainly have no way of knowing whether the caller is trained on the consent decree or whether they used methods not allowed by the consent decree. Can MPD receive information from Crime Stoppers?

Sent from my iPhone

EXHIBIT D

BUTLER | SNOW

August 29, 2019

VIA ELECTRONIC MAIL

R. Mark Glover, Esq.
Baker Donelson
Bearman, Caldwell & Berkowitz, PC
2000 First Tennessee Building
165 Madison Ave.
Memphis, TN 38103

Re: *ACLU-TN v. City of Memphis*, Case No. 2:17-cv-02120-JPM-jay:
August 28, 2019, Response to Court Direction re: Coordination Opinion

Dear Mark:

This letter responds to your email of Wednesday, August 28, 2019, a copy of which is enclosed. Both documents will be treated as sensitive and, as with earlier and similar correspondence of this kind, submitted directly to Judge McCalla to decide whether, and, if so, to what extent, they should be made public.

Your request to keep the Crime Stoppers program and the Multi-Agency Gang Unit in operation pending Judge McCalla's consideration of the City's soon-to-be-filed motion on their continuing viability under the *Kendrick* Consent Decree is granted.

With respect to the admissions process at City Hall, the interim process proposed by Mr. McMullen on August 22, 2019, may remain in place until the City obtains further guidance from the court. Will your soon-to-be-filed motion address this process?

With respect to your question about the PSP Symposium to be hosted by the City from September 9-11, 2019, I, like you, would like an opportunity to review the transcript from our *in camera* conference with the court at Tuesday's hearing. I continue to believe that § H of the consent decree prohibits the City from doing the following:

- sharing personal information collected in any way other than via lawful criminal investigation (as such information may not be maintained in the first instance); and

Post Office Box 171443
Memphis, TN 38187-1443

EDWARD L. STANTON III
901.680.7369
edward.stanton@butlersnow.com

Crescent Center
6075 Poplar Avenue, Suite 500
Memphis, TN 38119

T 901.680.7200 • F 901.680.7201 • www.butlersnow.com

BUTLER SNOW LLP

- sharing personal information collected via lawful criminal investigation unless such sharing is with another governmental law enforcement agency and that agency already is engaged in a lawful criminal investigation.

(Coordination Opinion, August 21, 2019, at 1.)

Likewise, in my view, § I of the consent decree prohibits the City from receiving any information from the FBI, the Secret Service, or any other law enforcement agencies unless the City first verifies that the information was not acquired in any way that the consent decree prohibits. (*See id.* at 2-3.)

My understanding from Tuesday's *in camera* conference on this subject is two-fold: First, I understand Judge McCalla to read §§ H and I the same way that I do. Second, I understand Judge McCalla to have authorized a limited, non-precedential departure from § I for purposes of providing security and public safety for the symposium. That departure allows the City to receive intelligence from the FBI, the Secret Service, and other law enforcement agencies without first verifying that such intelligence was acquired consistently with the consent decree's requirements. As your email correctly recites, this departure does not allow the City or the MPD to (1) request that other law enforcement agencies "plan or conduct any investigation, activity or conduct prohibited by th[e] [d]ecree," § I; or (2) act on any information the City receives that, on its face, reflects that it was acquired in some way that the consent decree prohibits.

I do not understand Judge McCalla to have authorized a departure from § H. In other words, in my view, the City and the MPD remain fully bound by § H as they prepare for and work with other law enforcement agencies before and during the symposium. They thus may share personal information with other law enforcement agencies, as opposed to receiving it from them, only as prescribed by § H.

I also should note that the example on which I understand Judge McCalla to have premised the City's limited, non-precedential departure from § I was an "active shooter" hypothetical scenario that you put forward. In my view, the City's ability to act in such a scenario is governed by § G of the Consent Decree rather than § I, because § G specifically concerns criminal investigations that "may result in the collection of information about the exercise of First Amendment rights, or interfere in any way with the exercise of such First Amendment rights." § G(1). I read § G to enable the City to conduct such investigations as it otherwise would as long as the investigations are approved and documented as § G requires. As a result, the MPD would not need a departure from § I to coordinate with other law enforcement agencies or otherwise act on an "active shooter" scenario because such action separately is authorized by § G—again, as long as the action is approved and documented as § G requires.

.

For this reason, please note that if, as a result of the limited, non-precedential departure from § I that Judge McCalla has authorized, the City receives information that it uses to begin or further a criminal investigation that may result in the collection of information about, or interfere with, the exercise of First Amendment rights, then that investigation will be subject to § G.

Finally, for purposes of establishing an open line of communication when the City anticipates receiving the information that has been authorized by Judge McCalla, please continue using the contact information that we provided via email on June 14, 2019, reproduced here for easy reference:

Name	Office Telephone	Email	Cellular Phone
Edward L. Stanton III	**(901) 680-7369**	**edward.stanton@butlersnow.com**	**(901) 302-7085**
Jim Letten	**(504) 299-7777**	**jim.letten@butlersnow.com**	**(504) 421-0020**
Gadson W. Perry	**(901) 680-7341**	**will.perry@butlersnow.com**	**(901) 494-6772**

Thank you for your time and attention to this matter.

Sincerely,

BUTLER SNOW LLP

Edward L. Stanton III

ES:tw

cc: Bruce A. McMullen, Esq. (via email only)
Jim Letten, Esq. (via email only)
Gadson W. Perry, Esq. (via email only)

49115179.v1

From: Glover, R. Mark [mailto:mglover@bakerdonelson.com]
Sent: Wednesday, August 28, 2019 9:48 AM
To: Edward L. Stanton III; Will Perry
Cc: McMullen, Bruce; Tullis, Mary Wu; Jill Silk; Saleem, Zayid-mem
Subject: Request For Monitor Approval or Advice

Ed,

Please treat this request as containing sensitive security information so that if it is to be submitted to the Court it will be done under circumstances which will allow the Court to determine whether to file it under seal as has been done with earlier and similar requests of this type.

While I have not yet obtained and reviewed the Court transcript from our in-chambers conference with His Honor, it is my understanding that for the purpose of the September 9-11 event, involving the convergence in Memphis of high level law enforcement officials from throughout the United States for a symposium, MPD is not prohibited from receiving intelligence from U. S. Secret Service, FBI or other federal law enforcement agencies which those agencies may gather (or may have already gathered) in order to provide security and protection for the attendees at this event, even though we will not be able to independently verify that such intelligence was gathered by those agencies in strict compliance with the guidelines that would govern MPD's own intelligence gathering as restricted and governed by the Kendrick Consent Decree. At the same time, we are also mindful that MPD may not make requests that those agencies conduct investigations as a surrogate for MPD or as a way to circumvent the Consent Decree's restrictions. We further understand that, even if gathered by federal governmental agencies, we would not be able to act on information which, on its face, demonstrates that it was collected for an inappropriate purpose. (We have no reason to expect that such would be the case.) Under those circumstances, we understand that MPD would be permitted to cooperate with those federal law enforcement agencies in providing security for the event and its attendees. We understand that this is a determination of the Court based upon the matter before it and does carry precedential value for other circumstances which have not yet been studied and passed upon by the Court. Please let us know if your understanding differs from ours so I can be sure I accurately advise my client.

We would be happy for the Monitor to have one of its law enforcement experts present 24 hours/day during the days when we anticipate receiving the type of information anticipated above, to be on site for discussions as issues arise or information is received; or to establish an open line of ongoing communication of some other kind to keep you fully apprised of the events as they unfold. Alternatively, we could provide appropriate MPD personnel for a debriefing by the Monitor at the conclusion of the event. Obviously we are open to suggestions of any other ways in which you would like to be kept fully informed as these activities occur.

We further understand that while the "Lobbyguard" photo system at City Hall is to remain unused

going forward, it was considered permissible to ask for identification for persons entering City Hall and to continue the use of the metal detector. Again, if I am mistaken on this point, please kindly correct me.

Our time before His Honor in chambers was limited, and although he did not give full consideration to issues which were raised concerning either the Multi-Agency Gang Unit or Crime Stoppers, we intend to file a motion under seal dealing with those, and perhaps other, discreet issues within the next few business days. It seems to me that considerations involving multi-law enforcement agency cooperation surrounding the Multi-Agency Gang Unit raise several issues similar to those involved in the Court's analysis of MPD receipt of information from other law enforcement agencies in connection with the September 9-11 event. Moreover, I believe there is recognition by everyone before the Bar in this case that we are in an interim or transition period pending final implementation of the policy and procedure revisions ordered by the Court and are feeling our way along in attempting to strike a balance to allow continuity of public safety while coming into compliance with the Consent Decree. For these reasons, we would respectfully request that we not be required to shut down these two programs pending Court consideration of our soon-to-be-filed motion on those subjects. Thank you for your time and consideration.

Mark Glover
Office Managing Shareholder
Baker, Donelson, Bearman,
Caldwell & Berkowitz, P.C.
165 Madison Avenue, Suite 2000
Memphis, TN 38103
Telephone: 901.577.2222
Facsimile: 901.577.0732
Email: mglover@bakerdonelson.com
www.bakerdonelson.com

Baker, Donelson, Bearman, Caldwell & Berkowitz, P.C.
represents clients across the U.S. and abroad from offices
in Alabama, Florida, Georgia, Louisiana, Mississippi, Tennessee,
Texas and Washington, D.C.

EXHIBIT E

Bureau of Justice Assistance

Award Title: FY 18 CGIC Program

Award Description:

The Local Law Enforcement Crime Gun Intelligence Center Integration (CGIC) Initiative, administered by BJA in partnership with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), is a competitive grant program that provides funding to state and local government entities that are experiencing precipitous increases in gun crime to implement comprehensive and holistic models to reduce violent crime and the illegal use of firearms within their jurisdictions by enabling them to integrate with their local ATF CGIC. The purpose of this initiative is to encourage local jurisdictions to work with their ATF partners to utilize intelligence, technology, and community engagement to swiftly identify firearms used unlawfully and their sources, and effectively prosecute perpetrators engaged in violent crime. The CGIC Initiative is part of the Project Safe Neighborhoods (PSN) Suite of programs, which is focused on reducing violent crime. The PSN Suite comprises PSN, Strategies for Policing Innovation, Innovative Prosecution Solutions, CGIC Initiative, National Public Safety Partnerships, Technology Innovation for Public Safety, Encouraging Innovation: Field Initiated, Innovations in Community-Based Crime Reduction, and Community Based Violence Prevention Demonstration, and these initiatives will coordinate proactively with the PSN team in the respective district of the United States Attorneys Office (USAO) to enhance collaboration and strengthen the commitment to reducing violent crime. Applicants must demonstrate this coordination with their USAO district PSN team in their submission.

The City of Memphis will use the BJA funds to enhance the analytical capabilities of the police department by hiring a contract analyst and eventually, a permanent senior crime analyst, as well as, purchasing technology to increase the capability to conduct investigations to identify, arrest, and prosecute violent gun crime offenders.

CA/NCF

Awardee Name: City of Memphis	**Award Number:** 2018-DG-BX-0004
Solicitation Title: BJA FY 18 Local Law Enforcement Crime Gun Intelligence Center Integration Initiative	**Fiscal Year:** 2018
Supplement Number: 00	**Amount:** $714,055.00
Earmark: No	**Recovery Act:** No
State/Territory: TN	**County:** Shelby
Congressional District: 09	**Award Status:** Open

EXHIBIT F

Bureau of Justice Assistance

Award Title: FY 18 TIPS - Memphis	
Award Description: The FY 2018 Technology Innovation for Public Safety (TIPS) Addressing Precipitous Increases in Crime is part of the Project Safe Neighborhoods (PSN) Suite of programs, which is focused on reducing violent crime. The TIPS Program is designed to enable strategic information sharing across crime-fighting agencies with identified partnerships to address specific local or regional crime problems. Often these efforts will require a multidisciplinary response involving law enforcement, analysts and/or investigators, information technology staff, public safety and/or first responders, adjudications and/or courts, corrections, human services organizations, and other stakeholders. The City of Memphis will use the BJA funds to increase the License Plate Reader (LPR) technology by securing six mobile brief case LPR systems to investigate violent gang crimes in their jurisdiction. During investigations, officers will greatly benefit from LPR technology to quickly be able to both read and store license plates for their cases. CA/NCF	
Awardee Name: City of Memphis	**Award Number:** 2018-DG-BX-K010
Solicitation Title: BJA FY 18 Technology Innovation for Public Safety (TIPS) Addressing Precipitous Increases in Crime	**Fiscal Year:** 2018
Supplement Number: 00	**Amount:** $417,224.00
Earmark: No	**Recovery Act:** No
State/Territory: TN	**County:** Shelby
Congressional District: 09	**Award Status:** Open

EXHIBIT G

28 CFR Part 23

CRIMINAL INTELLIGENCE SYSTEMS OPERATING POLICIES

Executive Order 12291

1998 Policy Clarification

1993 Revision and Commentary

28 CFR Part 23

Executive Order 12291

These regulations are not a "major rule" as defined by section 1(b) of Executive Order No. 12291, 3 CFR part 127 (1981), because they do not result in: (a) An effect on the economy of $100 million or more, (b) a major increase in any costs or prices, or (c) adverse effects on competition, employment, investment, productivity, or innovation among American enterprises.

Regulatory Flexibility Act

These regulations are not a rule within the meaning of the Regulatory Flexibility Act, 5 U.S.C. 601-612. These regulations, if promulgated, will not have a "significant" economic impact on a substantial number of small "entities," as defined by the Regulatory Flexibility Act.

Paperwork Reduction Act

There are no collection of information requirements contained in the proposed regulation.

List of Subjects in 28 CFR Part 23

Administrative practice and procedure, Grant programs, Intelligence, Law Enforcement.

For the reasons set out in the preamble, title 28, part 23 of the Code of Federal Regulations is revised to read as follows:

PART 23-CRIMINAL INTELLIGENCE SYSTEMS OPERATING POLICIES Sec.
23.1 Purpose.
23.2 Background.
23.3 Applicability.
23.20 Operating principles.
23.30 Funding guidelines.
23.40 Monitoring and auditing of grants for the funding of intelligence systems.
Authority: 42 U.S.C. 3782(a); 42 U.S.C. 3789g(c).

§ 23.1 Purpose.
The purpose of this regulation is to assure that all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, et seq., as amended (Pub. L. 90-351, as amended by Pub. L. 91-644, Pub. L. 93-83, Pub. L. 93-415, Pub. L. 94-430, Pub. L. 94-503, Pub. L. 95-115, Pub. L. 96-157, Pub. L. 98-473, Pub. L. 99-570, Pub. L. 100-690, and Pub. L. 101-647), are utilized in conformance with the privacy and constitutional rights of individuals.

§ 23.2 Background.
It is recognized that certain criminal activities including but not limited to loan sharking, drug trafficking, trafficking in stolen property, gambling, extortion, smuggling, bribery, and corruption of public officials often involve some degree of regular coordination and permanent organization involving a large number of participants over a broad geographical area. The exposure of such ongoing networks of criminal activity can be aided by the pooling of information about such activities. However, because the collection and exchange of intelligence data necessary to support control of serious criminal activity may represent potential threats to the privacy of individuals to whom such data relates, policy guidelines for Federally funded projects are required.

§ 23.3 Applicability.
(a) These policy standards are applicable to all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, et seq., as amended (Pub. L. 90-351, as amended by Pub. L. 91-644, Pub. L. 93-83, Pub. L. 93-415, Pub. L. 94-430, Pub. L. 94-503, Pub. L. 95-115, Pub. L. 96-157, Pub. L. 98-473, Pub. L. 99-570, Pub. L. 100-690, and Pub. L. 101-647).

(b) As used in these policies: (1) Criminal Intelligence System or Intelligence System means the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information; (2) Interjurisdictional Intelligence System

means an intelligence system which involves two or more participating agencies representing different governmental units or jurisdictions; (3) Criminal Intelligence Information means data which has been evaluated to determine that it: (i) is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and (ii) meets criminal intelligence system submission criteria; (4) Participating Agency means an agency of local, county, State, Federal, or other governmental unit which exercises law enforcement or criminal investigation authority and which is authorized to submit and receive criminal intelligence information through an interjurisdictional intelligence system. A participating agency may be a member or a nonmember of an interjurisdictional intelligence system; (5) Intelligence Project or Project means the organizational unit which operates an intelligence system on behalf of and for the benefit of a single agency or the organization which operates an interjurisdictional intelligence system on behalf of a group of participating agencies; and (6) Validation of Information means the procedures governing the periodic review of criminal intelligence information to assure its continuing compliance with system submission criteria established by regulation or program policy.

§ 23.20 Operating principles.
(a) A project shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.

(b) A project shall not collect or maintain criminal intelligence information about the political, religious or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.

(c) Reasonable Suspicion or Criminal Predicate is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise. In an interjurisdictional intelligence system, the project is responsible for establishing the existence of reasonable suspicion of criminal activity either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.

(d) A project shall not include in any criminal intelligence system information which has been obtained in violation of any applicable Federal, State, or local law or ordinance. In an interjurisdictional intelligence system, the project is responsible for establishing that no information is entered in violation of Federal, State, or local laws, either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.

(e) A project or authorized recipient shall disseminate criminal intelligence information only where there is a need to know and a right to know the information in the performance of a law enforcement activity.

(f) (1) Except as noted in paragraph (f)(2) of this section, a project shall disseminate criminal intelligence information only to law enforcement authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination which are consistent with these principles.

(2) Paragraph (f)(1) of this section shall not limit the dissemination of an assessment of criminal intelligence information to a government official or to any other individual, when necessary, to avoid imminent danger to life or property.

(g) A project maintaining criminal intelligence information shall ensure that administrative, technical, and physical safeguards (including audit trails) are adopted to insure against unauthorized access and against intentional or unintentional damage. A record indicating who has been given information, the reason for release of the information, and the date of each dissemination outside the project shall be kept. Information shall be labeled to indicate levels of sensitivity, levels of confidence, and the identity of submitting agencies and control officials. Each project must establish written definitions for the need to know and right to know standards for dissemination to other agencies as provided in paragraph (e) of this section. The project is responsible for establishing the existence of an inquirer's need to know and right to know the information being requested either through inquiry or by delegation of this responsibility to a properly trained

participating agency which is subject to routine inspection and audit procedures established by the project. Each intelligence project shall assure that the following security requirements are implemented:

(1) Where appropriate, projects must adopt effective and technologically advanced computer software and hardware designs to prevent unauthorized access to the information contained in the system;

(2) The project must restrict access to its facilities, operating environment and documentation to organizations and personnel authorized by the project;

(3) The project must store information in the system in a manner such that it cannot be modified, destroyed, accessed, or purged without authorization;

(4) The project must institute procedures to protect criminal intelligence information from unauthorized access, theft, sabotage, fire, flood, or other natural or manmade disaster;

(5) The project must promulgate rules and regulations based on good cause for implementing its authority to screen, reject for employment, transfer, or remove personnel authorized to have direct access to the system; and

(6) A project may authorize and utilize remote (off-premises) system data bases to the extent that they comply with these security requirements.

(h) All projects shall adopt procedures to assure that all information which is retained by a project has relevancy and importance. Such procedures shall provide for the periodic review of information and the destruction of any information which is misleading, obsolete or otherwise unreliable and shall require that any recipient agencies be advised of such changes which involve errors or corrections. All information retained as a result of this review must reflect the name of the reviewer, date of review and explanation of decision to retain. Information retained in the system must be reviewed and validated for continuing compliance with system submission criteria before the expiration of its retention period, which in no event shall be longer than five (5) years.

(i) If funds awarded under the Act are used to support the operation of an intelligence system, then:

(1) No project shall make direct remote terminal access to intelligence information available to system participants, except as specifically approved by the Office of Justice Programs (OJP) based on a determination that the system has adequate policies and procedures in place to insure that it is accessible only to authorized systems users; and

(2) A project shall undertake no major modifications to system design without prior grantor agency approval.

(j) A project shall notify the grantor agency prior to initiation of formal information exchange procedures with any Federal, State, regional, or other information systems not indicated in the grant documents as initially approved at time of award.

(k) A project shall make assurances that there will be no purchase or use in the course of the project of any electronic, mechanical, or other device for surveillance purposes that is in violation of the provisions of the Electronic Communications Privacy Act of 1986, Public Law 99-508, 18 U.S.C. 2510-2520, 2701-2709 and 3121-3125, or any applicable State statute related to wiretapping and surveillance.

(l) A project shall make assurances that there will be no harassment or interference with any lawful political activities as part of the intelligence operation.

(m) A project shall adopt sanctions for unauthorized access, utilization, or disclosure of information contained in the system.

(n) A participating agency of an interjurisdictional intelligence system must maintain in its agency files information which documents each submission to the system and supports compliance with project entry criteria. Participating agency files supporting system submissions must be made available for reasonable audit and inspection by project representatives. Project representatives will conduct participating agency inspection and audit in such a manner so as to protect the confidentiality and sensitivity of participating agency intelligence records.

(o) The Attorney General or designee may waive, in whole or in part, the applicability of a particular requirement or requirements contained in this part with respect to a criminal intelligence system, or for a class of submitters or users of such system, upon a clear and convincing showing that such waiver would enhance the collection, maintenance or dissemination of information in the criminal intelligence system, while ensuring that such system would not be utilized in violation of the privacy and constitutional rights of individuals or any applicable state or federal law.

§ 23.30 Funding guidelines.
The following funding guidelines shall apply to all Crime Control Act funded discretionary assistance awards and Bureau of Justice Assistance (BJA) formula grant program subgrants, a purpose of which is to support the operation of an intelligence system. Intelligence systems shall only be funded where a grantee/subgrantee agrees to adhere to the principles set forth above and the project meets the following criteria:

(a) The proposed collection and exchange of criminal intelligence information has been coordinated with and will support ongoing or proposed investigatory or prosecutorial activities relating to specific areas of criminal activity.

(b) The areas of criminal activity for which intelligence information is to be utilized represent a significant and recognized threat to the population and:

(1) Are either undertaken for the purpose of seeking illegal power or profits or pose a threat to the life and property of citizens; and

(2) Involve a significant degree of permanent criminal organization; or

(3) Are not limited to one jurisdiction.

(c) The head of a government agency or an individual with general policy making authority who has been expressly delegated such control and supervision by the head of the agency will retain control and supervision of information collection and dissemination for the criminal intelligence system. This official shall certify in writing that he or she takes full responsibility and will be accountable for the information maintained by and disseminated from the system and that the operation of the system will be in compliance with the principles set forth in § 23.20.

(d) Where the system is an interjurisdictional criminal intelligence system, the governmental agency which exercises control and supervision over the operation of the system shall require that the head of that agency or an individual with general policymaking authority who has been expressly delegated such control and supervision by the head of the agency:

(1) assume official responsibility and accountability for actions taken in the name of the joint entity, and

(2) certify in writing that the official takes full responsibility and will be accountable for insuring that the information transmitted to the interjurisdictional system or to participating agencies will be in compliance with the principles set forth in § 23.20.

The principles set forth in § 23.20 shall be made part of the by-laws or operating procedures for that system. Each participating agency, as a condition of participation, must accept in writing those principles which govern the submission, maintenance and dissemination of information included as part of the interjurisdictional system.

(e) Intelligence information will be collected, maintained and disseminated primarily for State and local law enforcement efforts, including efforts involving Federal participation.

§ 23.40 Monitoring and auditing of grants for the funding of intelligence systems.

(a) Awards for the funding of intelligence systems will receive specialized monitoring and audit in accordance with a plan designed to insure compliance with operating principles as set forth in § 23.20. The plan shall be approved prior to award of funds.

(b) All such awards shall be subject to a special condition requiring compliance with the principles set forth in § 23.20.

(c) An annual notice will be published by OJP which will indicate the existence and the objective of all systems for the continuing interjurisdictional exchange of criminal intelligence information which are subject to the 28 CFR Part 23 Criminal Intelligence Systems Policies.

Laurie Robinson
Acting Assistant Attorney General
Office of Justice Programs
(FR Doc. 93-22614 Filed 9-15-93; 8:45 am)

Criminal Intelligence Sharing Systems; Policy Clarification

[Federal Register: December 30, 1998 (Volume 63, Number 250)]
[Page 71752-71753]
From the Federal Register Online via GPO Access [wais.access.gpo.gov]
DEPARTMENT OF JUSTICE
28 CFR Part 23
[OJP(BJA)-1177B]
RIN 1121-ZB40

1993 Revision and Commentary

28 CFR Part 23

Final Revision to the Office of Justice Programs, Criminal Intelligence Systems Operating Policies

---

AGENCY: Office of Justice Programs, Justice.

ACTION: Final Rule

SUMMARY: The regulation governing criminal intelligence systems operating through support under Title I of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, is being revised to update basic authority citations and nomenclature, to clarify the applicability of the regulation, to define terms, and to modify a number of the regulation's operating policies and funding guidelines.

EFFECTIVE DATE: September 16, 1993

FOR FURTHER INFORMATION CONTACT: Paul Kendall, Esquire, General Counsel, **Office of Justice Programs**, 633 Indiana Ave., NW., Suite 1245-E, Washington, DC 20531, Telephone (202) 307-6235.

SUPPLEMENTARY INFORMATION: The rule which this rule supersedes had been in effect and unchanged since September 17, 1980. A notice of proposed rulemaking for 28 CFR part 23, was published in the Federal Register on February 27, 1992, (57 FR 6691).

The statutory authorities for this regulation are section 801(a) and section 812(c) of title I of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, (the Act), 42 U.S.C. 3782(a) and 3789g(c). 42 U.S.C. 3789g (c) and (d) provide as follows:

Confidentiality of Information

Sec. 812....

(c) All criminal intelligence systems operating through support under this title shall collect, maintain, and disseminate criminal intelligence information in conformance with policy standards which are prescribed by the Office of Justice Programs and which are written to assure that the funding and operation of these systems furthers the purpose of this title and to assure that such systems are not utilized in violation of the privacy and constitutional rights of individuals.

(d) Any person violating the provisions of this section, or of any rule, regulation, or order issued thereunder, shall be fined not to exceed $10,000, in addition to any other penalty imposed by law.

This statutory provision and its implementing regulation apply to intelligence systems funded under title I of the Act, whether the system is operated by a single law enforcement agency, is an interjurisdictional intelligence system, is funded with discretionary grant funds, or is funded by a State with formula grant funds awarded under the Act's Drug Control and System Improvement Grant Program pursuant to part E, subpart 1 of the Act, 42 U.S.C. 3751-3759.

The need for change to 28 CFR part 23 grew out of the program experience of the Office of Justice Programs (OJP) and its component agency, the Bureau of Justice Assistance (BJA), with the regulation and the changing and expanding law enforcement agency need to respond to criminal mobility, the National drug program, the increased complexity of criminal networks and conspiracies, and the limited funding available to State and local law enforcement agencies. In addition, law enforcement's capability to perform intelligence data base and analytical functions has been enhanced by technological advancements and sophisticated analytical techniques.

28 CFR part 23 governs the basic requirements of the intelligence system process. The process includes:

1. Information submission or collection
2. Secure storage
3. Inquiry and search capability
4. Controlled dissemination
5. Purge and review process

Information systems that receive, store and disseminate information on individuals or organizations based on reasonable suspicion of their involvement in criminal activity are criminal intelligence systems under the regulation. The definition includes both systems that store detailed intelligence or investigative information on the suspected criminal activities of subjects and those which store only information designed to identify individuals or organizations that are the subject of an inquiry or analysis (a so-called "pointer system"). It does not include criminal history record information or identification (fingerprint) systems.

There are nine significant areas of change to the regulation:

(1) Nomenclature changes (authority citations, organizational names) are included to bring the regulation up to date.

(2) Definitions of terms (28 CFR 23.3(b)) are modified or added as appropriate. The term "intelligence system" is redefined to clarify the fact that historical telephone toll files, analytical information, and work products that are not either retained, stored, or exchanged and criminal history record information or identification (fingerprint) systems are excluded from the definition, and hence are not covered by the regulation; the terms "interjurisdictional intelligence system", "criminal intelligence information", "participating agency", "intelligence project", and "validation of information" are key terms that are defined in the regulation for the first time.

(3) The operating principles for intelligence systems (28 CFR 23.20) are modified to define the term "reasonable suspicion" or "criminal predicate". The finding of reasonable suspicion is a threshold requirement for entering intelligence information on an individual or organization into an intelligence data base (28 CFR 23.20(c)). This determination, as well as determinations that information was legally obtained (28 CFR 23.20(d)) and that a recipient of the information has a need to know and a right to know the information in the performance of a law enforcement function (28 CFR 23.20(e)), are established as the responsibility of the project for an interjurisdictional intelligence system. However, the regulation permits these responsibilities to be delegated to a properly trained participating agency which is subject to project inspection and audit (28 CFR 23.20(c),(d),(g)).

(4) Security requirements are established to protect the integrity of the intelligence data base and the information stored in the data base (28 CFR 23.20(g)(1)(i)-(vi)).

(5) The regulation provides that information retained in the system must be reviewed and validated for continuing compliance with system submission criteria within a 5-year retention period. Any information not validated within that period must be purged from the system (28 CFR 23.20(h)).

(6) Another change continues the general prohibition of direct remote terminal access to intelligence information in a funded intelligence system but provides an exception for systems which obtain express OJP approval based on a determination that the system has adequate policies and procedures in place to insure that access to system intelligence information is limited to authorized system users (28 CFR 23.20(i)(1)). OJP will carefully review all requests for exception to assure that a need exists and that system integrity will be provided and maintained (28 CFR 23.20(i)(1)).

(7) The regulation requires participating agencies to maintain back-up files for information submitted to an interjurisdictional intelligence system and provide for inspection and audit by project staff (28 CFR 23.20(h)).

(8) The final rule also includes a provision allowing the Attorney General or the Attorney General's designee to authorize a departure from the specific requirements of this part, in those cases where it is clearly shown that such waiver would promote the purposes and effectiveness of a criminal intelligence system while at the same time ensuring compliance with all applicable laws and protection for the privacy and constitutional

rights of individuals. The Department recognizes that other provisions of federal law may be applicable to (or may be adopted in the future with respect to) certain submitters or users of information in criminal intelligence systems. Moreover, as technological developments unfold over time in this area, experience may show that particular aspects of the requirements in this part may no longer be needed to serve their intended purpose or may even prevent desirable technological advances. Accordingly, this provision grants the flexibility to make such beneficial adaptations in particular cases or classes without the necessity to undertake a new rulemaking process. This waiver authority could only be exercised by the Attorney General or designee, in writing, upon a clear and convincing showing (28 CFR 23.20 (o)).

(9) The funding guidelines (28 CFR 23.30) are revised to permit funded intelligence systems to collect information either on organized criminal activity that represents a significant and recognized threat to the population or on criminal activity that is multi-jurisdictional in nature.

Rulemaking History

On February 27, 1992, the Department of Justice, Office of Justice Programs, published a notice of proposed rulemaking in the Federal Register (57 FR 6691).

The Office of Justice Programs received a total of eleven comments on the proposed regulation, seven from State agencies, two from Regional Information Sharing Systems (RISS) program fund recipients, one from a Federal agency, and one from the RISS Project Directors Association. Comments will be discussed in the order in which they address the substance of the proposed regulation.

Discussion of Comments

Title - Part 23
Comment: One commentor suggested reinserting the word "Operating" in the title of the regulation to read "Criminal Intelligence Systems Operating Policies" to reflect that the regulation applies only to policies governing system operations.

Response: Agreed. The title has been changed.

APPLICABILITY - SECTION 23.3(a)
Comment: A question was raised by one respondent as to whether the applicability of the regulation under Section 23.3(a) to systems "operating through support" under the Crime Control Act included agencies receiving any assistance funds and who operated an intelligence system or only those who received assistance funds for the specific purpose of funding the operation of an intelligence system.

Response: The regulation applies to grantees and subgrantees who receive and use Crime Control Act funds to fund the operation of an intelligence system.

Comment: Another commentor asked whether the purchase of software, office equipment, or the payment of staff salaries for a criminal intelligence system would constitute "operating through support" under the Crime Control Act.

Response: Any direct Crime Control Act fund support that contributes to the operation of a criminal intelligence system would subject the system to the operation of the policy standards during the period of fund support.

Comment: A third commentor inquired whether an agency's purchase of a telephone pen register or computer equipment to store and analyze pen register information would subject the agency or its information systems to the regulation.

Response: No, neither a pen register nor equipment to analyze telephone toll information fall under the definition of a criminal intelligence system even though they may assist an agency to produce investigative or other information for an intelligence system.

APPLICABILITY - SECTION 23.3(b)
Comment: Several commentors questioned whether information systems that are designed to collect information on criminal suspects for purposes of inquiry and analysis, and which provide for dissemination of such information, qualify as "criminal intelligence systems." One pointed out that the information qualifying for system submission could not be "unconfirmed" or "soft" intelligence. Rather, it would generally have to be

investigative file-based information to meet the "reasonable suspicion" test.

Response: The character of an information system as a criminal intelligence system does not depend upon the source or categorization of the underlying information as "raw" or "soft" intelligence, preliminary investigation information, or investigative information, findings or determinations. It depends upon the purpose for which the information system exists and the type of information it contains. If the purpose of the system is to collect and share information with other law enforcement agencies on individuals reasonably suspected of involvement in criminal activity, and the information is identifying or descriptive information about the individual and the suspected criminal activity, then the system is a criminal intelligence system for purposes of the regulation. Only those criminal intelligence systems that receive, store and provide for the interagency exchange and analysis of criminal intelligence information in a manner consistent with this regulation are eligible for funding support with Crime Control Act funds.

Comment: One respondent asked whether the definition of criminal intelligence system covered criminal history record information (CHRI) systems, fugitive files, or other want or warrant based information systems.

Response: No. A CHRI system contains information collected on arrests, detention, indictments, informations or other charges, dispositions, sentencing, correctional supervision, and release. It encompasses systems designed to collect, process, preserve, or disseminate such information.

CHRI is factual, historical and objective information which provides a criminal justice system "profile" of an individual's past and present involvement in the criminal justice system. A fugitive file is designed to provide factual information to assist in the arrest of individuals for whom there is an outstanding want or warrant. Criminal intelligence information, by contrast, is both factual and conjectural (reasonable suspicion), current and subjective. It is intended for law enforcement use only, to provide law enforcement officers and agencies with useful information on criminal suspects and to foster interagency coordination and cooperation. A criminal intelligence system can have criminal history record information in it as an identifier but a CHRI system would not contain the suspected criminal activity information contained in a criminal intelligence system.

This distinction provides the basis for the limitations on criminal intelligence systems set forth in the operating policies. Because criminal intelligence information is both conjectural and subjective in nature, may be widely disseminated through the interagency exchange of information and cannot be accessed by criminal suspects to verify that the information is accurate and complete, the protections and limitations set forth in the regulation are necessary to protect the privacy interests of the subjects and potential subjects of a criminal intelligence system.

Comment: Another commentor asked whether a law enforcement agency's criminal intelligence information unit, located at headquarters, which authorizes no outside access to information in its intelligence system, would be subject to the regulation.

Response: No. The sharing of investigative or general file information on criminal subjects within an agency is a practice that takes place on a daily basis and is necessary for the efficient and effective operation of a law enforcement agency. Consequently, whether such a system is described as a case management or intelligence system, the regulation is not intended to apply to the exchange or sharing of such information when it takes place within a single law enforcement agency or organizational entity. For these purposes, an operational multi-jurisdictional task force would be considered a single organizational entity provided that it is established by and operates under a written memorandum of understanding or interagency agreement. The definition of "Criminal Intelligence System" has been modified to clarify this point. However, if a single agency or entity system provides access to system information to outside agencies on an inquiry or request basis, as a matter of either policy or practice, the system would qualify as a criminal intelligence system and be subject to the regulation.

Comment: A commentor questioned whether the proposed exclusion of "analytical information and work products" from the definition of "Intelligence System" was intended to exclude all dissemination of analytical results from coverage under the regulation.

Response: No. The exceptions in the proposed definition of "Intelligence System" of modus operandi files, historical telephone toll files and analytical information and work products are potentially confusing. The exceptions reflect types of data that may or may not qualify as "Criminal Intelligence Information" depending on particular facts and circumstances. Consequently, these exceptions have been deleted from the definition

of "Intelligence System" in the final rule. For example, analytical information and work products that are derived from unevaluated or bulk data (i.e. information that has not been tested to determine that it meets intelligence system submission criteria) are not intelligence information if they are returned to the submitting agency. This information and its products cannot be retained, stored, or made available for dissemination in an intelligence system unless and until the information has been evaluated and determined to meet system submission criteria. The proposed definition of "Analytical Information and Work Products" in Section 23.3(b) has also been deleted.

To address the above issues, the definition of "Intelligence System" has been modified to define a "Criminal Intelligence System or Intelligence System" to mean "the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information."

Comment: Several commentors raised questions regarding the concept of "evaluated data" in the definition of "Criminal Intelligence Information", requesting guidance on what criteria to use in evaluating data. Another questioned whether there needed to be an active investigation as the basis for information to fall within the definition and whether information on an individual who or organization which is not the primary subject or target of an investigation or other data source, e.g. a criminal associate or co-conspirator, can qualify as "Criminal Intelligence Information."

Response: The definition of "Criminal Intelligence Information" has been revised to reflect that data is evaluated for two purposes related to criminal intelligence system submissions: (1) to determine that it is relevant in identifying a criminal suspect and the criminal activity involved; and (2) to determine that the data meets criminal intelligence system submission criteria, including reasonable suspicion of involvement in criminal activity. As rewritten, there is no requirement that an "active investigation" is necessary. Further, the revised language makes it clear that individuals or organizations who are not primary subjects or targets can be identified in the criminal intelligence information, provided that they independently meet system submission criteria.

Comment: One commentor requested clarification of the role of the "Project" in the operation of an intelligence system, i.e. is the project required to have physical control (possession) of the information in an intelligence system or will authority over the system (operational control) suffice?

Response: Operational control over an intelligence system's intelligence information is sufficient. The regulation seeks to establish a single locus of authority and responsibility for system information. Once that principle is established, the regulation permits, for example, the establishment of remote (off premises) data bases that meet applicable security requirements.

OPERATING PRINCIPLES - SECTION 23.20(c)

Comment: One respondent took the position that "Reasonable Suspicion", as defined in Section 23.20 (c), is not necessary to the protection of individual privacy and Constitutional rights, suggesting instead that information in a funded intelligence system need only be "necessary and relevant to an agency's lawful purposes."

Response: While it is agreed that the standard suggested is appropriate for investigative or other information files maintained for use by or within an agency, the potential for national dissemination of information in intelligence information systems, coupled with the lack of access by subjects to challenge the information, justifies the reasonable suspicion standard as well as other operating principle restrictions set forth in this regulation. Also, the quality and utility of "hits" in an information system is enhanced by the reasonable suspicion requirement. Scarce resources are not wasted by agencies in coordinating information on subjects for whom information is vague, incomplete and conjectural.

Comment: The prior commentor also criticized the proposed definition of reasonable suspicion for its specific reference to an "investigative file" as the source of intelligence system information, the potential inconsistency between the concepts of "infer" and "conclude" as standards for determining whether reasonable suspicion is justified by the information available, and the use of "reasonable possibility" rather than "articulable" or "sufficient" facts as the operative standard to conclude that reasonable suspicion exists.

Response: The reference to an "investigative file" as the information source has been broadened to encompass any information source. The information available must provide a basis for the submitter to "believe" there is a reasonable possibility of the subject's involvement in the criminal activity or enterprise.

The concept of a "basis to believe" requires reasoning and logic coupled with sound judgment based on experience in law enforcement rather than a mere hunch, whim, or guess. The belief that is formed, that there is a "reasonable possibility" of criminal involvement, has been retained because the proposed standard is appropriately less restrictive than that which is required to establish probable cause.

OPERATING PRINCIPLES - SECTION 23.20(d)

Comment: Section 23.20(d) prohibits the inclusion in an intelligence system of information obtained in violation of Federal, State, or local law or ordinance. Would a project be potentially liable for accepting, maintaining and disseminating such information even if it did not know that the information was illegally obtained?

Response: In addition to protecting the rights of individuals and organizations that may be subjects in a criminal intelligence system, this prohibition serves to protect a project from liability for disseminating illegally obtained information. A clear project policy that prohibits the submission of illegally obtained information, coupled with an examination of supporting information to determine that the information was obtained legally or the delegation of such authority to a properly trained participating agency, and the establishment and performance of routine inspection and audit of participating agency records, should be sufficient to shield a project from potential liability based on negligence in the performance of its intelligence information screening function.

OPERATING PRINCIPLES - SECTION 23.20(h)

Comment: One commentor requested clarification of the "periodic review" requirement in Section 23.20(h) and what constitutes an "explanation of decision to retain" information.

Response: The periodic review requirement is designed to insure that system information is accurate and as up-to-date as reasonably possible. When a review has occurred, the record is appropriately updated and notated. The explanation of decision to retain can be a variety of reasons including "active investigation", "preliminary review in progress", "subject believed still active in jurisdiction", and the like. When information that has been reviewed or updated and a determination made that it continues to meet system submission criteria, the information has been "validated" and begins a new retention period. The regulation limits the retention period to a maximum of five years without a review and validation of the information.

OPERATING PRINCIPLES - SECTION 23.20(i)

Comment: One commentor requested a definition of "remote terminal" and asked how OJP would determine whether "adequate policies and procedures" are in place to insure the continued integrity of a criminal intelligence system.

Response: A "remote terminal" is hardware that enables a participating agency to input into or access information from a project's criminal intelligence data base without the intervention of project staff. While the security requirements set forth in Section 23.20(g)(1)-(5) should minimize the threat to system integrity from unauthorized access to and the use of system information, special measures are called for when direct remote terminal access is authorized.

The Office of Justice Programs will expect any request for approval of remote terminal access to include information on the following system protection measures:

1. Procedures for identification of authorized remote terminals and security of terminals;

2. Authorized access officer (remote terminal operator) identification and verification procedures;

3. Provisions for the levels of dissemination of information as directed by the submitting agency;

4. Provisions for the rejection of submissions unless critical data fields are completed;

5. Technological safeguards on system access, use, dissemination, and review and purge;

6. Physical security of the system;

7. Training and certification of system-participating agency personnel;

8. Provisions for the audit of system-participating agencies, to include: file data supporting submissions to the system; security of access terminals; and policy and procedure compliance; and

9. Documentation for audit trails of the entire system operation.

Moreover, a waiver provision has been added to ensure flexibility in adapting quickly to technological and legal changes which may impact any of the requirements contained in this regulation. See Section 23.20 (o).

Comment: Related to the above discussion, another commentor asked whether restrictions on direct remote terminal access would prohibit remote access to an "index" of information in the system.

Response: Yes. The ability to obtain all information directly from a criminal intelligence system through the use of hardware based outside the system constitutes direct remote terminal access contrary to the provisions of Section 23.20(i)(1), except as specifically approved by OJP. Thus, a hit/no hit response, if gleaned from an index, would bring a remote terminal within the scope of the requirement for OJP approval of direct remote terminal access.

Comment: One commentor pointed out that the requirement for prior OJP approval of "modifications to system design" was overly broad and could be read to require that even minor changes be submitted for approval. The commentor proposed a substitute which would limit the requirement to those modifications "that alter the system's identified goals in a way contrary to the requirements of (this regulation)."

Response: While it is agreed that the language is broad, the proposed limitation is too restrictive. The intent was that "modifications to system design" refer to "major" changes to the system, such as the nature of the information collected, the place or method of information storage, the authorized uses of information in the system, and provisions for access to system information by authorized participating agencies. This clarification has been incorporated in the regulation. In order to decentralize responsibility for approval of system design modifications, the proposed regulation has been revised to provide for approval of such modifications by the grantor agency rather than OJP. A similar change has been made to Section 23.20(j).

OPERATING PRINCIPLES - SECTION 23.20(n)

Comment: Several commentors expressed concern with the verification procedures set forth in Section 23.20(n). One suggested that file information cannot "verify" the correctness of submissions but instead serves to "document" or "substantiate" its correctness. Another proposed deleting the requirements that (1) files maintained by participating agencies to support system submissions be subject to the operating principles, and (2) participating agencies are authorized to maintain such files separately from other agency files. The first requirement conflicts with the normal investigative procedures of a law enforcement agency in that all information in agency source files cannot meet the operating principles, particularly the reasonable suspicion and relevancy requirements. The important principle is that the information which is gleaned from an agency's source files and submitted to the system meet the operating principles. The second requirement has no practical value. At most, it results in the creation of duplicative files or in submission information being segregated from source files.

Response: OJP agrees with both comments. The word "documents" has been substituted for "verifies" and the provisions subjecting participating agency source files to the operating principles and authorizing maintenance of separate files have been deleted. Projects should use their audit and inspection access to agency source files to document the correctness of participating agency submissions on a sample basis.

FUNDING GUIDELINES - SECTION 23.30(b)

Comment: One commentor asked: Who defines the areas of criminal activity that "represent a significant and recognized threat to the population?"

Response: The determination of areas of criminal activity focus and priority are matters for projects, project policy boards and member agencies to determine, provided that the additional regulatory requirements set forth in Section 23.30(b) are met.

MONITORING AND AUDITING OF GRANTS - SECTION 23.40(a)

Comment: One commentor asked: "Who is responsible for developing the specialized monitoring and audit of awards for intelligence systems to insure compliance with the operating principles"?

Response: The grantor agency (the agency awarding a sub-grant to support an intelligence system) shall establish and approve a plan for specialized monitoring and audit of sub-awards prior to award. For the BJA Formula Grant Program, the State agency receiving the award from BJA is the grantor agency. Technical assistance and support in establishing a monitoring and audit plan is available through BJA.

INFORMATION ON JUVENILES

Comment: Can intelligence information pertaining to a juvenile who otherwise meets criminal intelligence system submission criteria be entered into an intelligence data base?

Response: There is no limitation or restriction on entering intelligence information on juvenile subjects set forth in Federal law or regulation. However, State law may restrict or prohibit the maintenance or dissemination of such information by its law enforcement agencies. Therefore, State laws should be carefully reviewed to determine their impact on this practice and appropriate project policies adopted.

Executive Order 12291
These regulations are not a "major rule" as defined by section 1(b) of Executive Order No. 12291, 3 CFR part 127 (1981), because they do not result in: (a) An effect on the economy of $100 million or more, (b) a major increase in any costs or prices, or (c) adverse effects on competition, employment, investment, productivity, or innovation among American enterprises.

Regulatory Flexibility Act
These regulations are not a rule within the meaning of the Regulatory Flexibility Act, 5 U.S.C. 601-612. These regulations, if promulgated, will not have a "significant" economic impact on a substantial number of small "entities," as defined by the Regulatory Flexibility Act.

Paperwork Reduction Act
There are no collection of information requirements contained in the proposed regulation.

List of Subjects in 28 CFR Part 23
Administrative practice and procedure, Grant programs, Intelligence, Law Enforcement.

For the reasons set out in the preamble, title 28, part 23 of the Code of Federal Regulations is revised to read as follows:

PART 23--CRIMINAL INTELLIGENCE SYSTEMS OPERATING POLICIES Sec.

1. Purpose.
2. Background.
3. Applicability.
4. Operating principles.
5. Funding guidelines.
6. Monitoring and auditing of grants for the funding of intelligence systems.

Authority: 42 U.S.C. 3782(a); 42 U.S.C. 3789g(c).

§ 23.1 Purpose.
The purpose of this regulation is to assure that all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, et seq., as amended (Pub. L. 90-351, as amended by Pub. L. 91-644, Pub. L. 93-83, Pub. L. 93-415, Pub. L. 94-430, Pub. L. 94-503, Pub. L. 95-115, Pub. L. 96-157, Pub. L. 98-473, Pub. L. 99-570, Pub. L. 100-690, and Pub. L. 101-647), are utilized in conformance with the privacy and constitutional rights of individuals.

§ 23.2 Background.
It is recognized that certain criminal activities including but not limited to loan sharking, drug trafficking, trafficking in stolen property, gambling, extortion, smuggling, bribery, and corruption of public officials often involve some degree of regular coordination and permanent organization involving a large number of participants over a broad geographical area. The exposure of such ongoing networks of criminal activity can

be aided by the pooling of information about such activities. However, because the collection and exchange of intelligence data necessary to support control of serious criminal activity may represent potential threats to the privacy of individuals to whom such data relates, policy guidelines for Federally funded projects are required.

§ 23.3 Applicability.
(a) These policy standards are applicable to all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, et seq., as amended (Pub. L. 90-351, as amended by Pub. L. 91-644, Pub. L. 93-83, Pub. L. 93-415, Pub. L. 94-430, Pub. L. 94-503, Pub. L. 95-115, Pub. L. 96-157, Pub. L. 98-473, Pub. L. 99-570, Pub. L. 100-690, and Pub. L. 101-647).

(b) As used in these policies: (1) Criminal Intelligence System or Intelligence System means the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information; (2) Interjurisdictional Intelligence System means an intelligence system which involves two or more participating agencies representing different governmental units or jurisdictions; (3) Criminal Intelligence Information means data which has been evaluated to determine that it: (i) is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and (ii) meets criminal intelligence system submission criteria; (4) Participating Agency means an agency of local, county, State, Federal, or other governmental unit which exercises law enforcement or criminal investigation authority and which is authorized to submit and receive criminal intelligence information through an interjurisdictional intelligence system. A participating agency may be a member or a nonmember of an interjurisdictional intelligence system; (5) Intelligence Project or Project means the organizational unit which operates an intelligence system on behalf of and for the benefit of a single agency or the organization which operates an interjurisdictional intelligence system on behalf of a group of participating agencies; and (6) Validation of Information means the procedures governing the periodic review of criminal intelligence information to assure its continuing compliance with system submission criteria established by regulation or program policy.

§ 23.20 Operating principles.
(a) A project shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.

(b) A project shall not collect or maintain criminal intelligence information about the political, religious or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.

(c) Reasonable Suspicion or Criminal Predicate is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise. In an interjurisdictional intelligence system, the project is responsible for establishing the existence of reasonable suspicion of criminal activity either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.

(d) A project shall not include in any criminal intelligence system information which has been obtained in violation of any applicable Federal, State, or local law or ordinance. In an interjurisdictional intelligence system, the project is responsible for establishing that no information is entered in violation of Federal, State, or local laws, either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.

(e) A project or authorized recipient shall disseminate criminal intelligence information only where there is a need to know and a right to know the information in the performance of a law enforcement activity.

(f) (1) Except as noted in paragraph (f) (2) of this section, a project shall disseminate criminal intelligence

information only to law enforcement authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination which are consistent with these principles.

(2) Paragraph (f) (1) of this section shall not limit the dissemination of an assessment of criminal intelligence information to a government official or to any other individual, when necessary, to avoid imminent danger to life or property.

(g) A project maintaining criminal intelligence information shall ensure that administrative, technical, and physical safeguards (including audit trails) are adopted to insure against unauthorized access and against intentional or unintentional damage. A record indicating who has been given information, the reason for release of the information, and the date of each dissemination outside the project shall be kept. Information shall be labeled to indicate levels of sensitivity, levels of confidence, and the identity of submitting agencies and control officials. Each project must establish written definitions for the need to know and right to know standards for dissemination to other agencies as provided in paragraph (e) of this section. The project is responsible for establishing the existence of an inquirer's need to know and right to know the information being requested either through inquiry or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project. Each intelligence project shall assure that the following security requirements are implemented:

(1) Where appropriate, projects must adopt effective and technologically advanced computer software and hardware designs to prevent unauthorized access to the information contained in the system;

(2) The project must restrict access to its facilities, operating environment and documentation to organizations and personnel authorized by the project;

(3) The project must store information in the system in a manner such that it cannot be modified, destroyed, accessed, or purged without authorization;

(4) The project must institute procedures to protect criminal intelligence information from unauthorized access, theft, sabotage, fire, flood, or other natural or manmade disaster;

(5) The project must promulgate rules and regulations based on good cause for implementing its authority to screen, reject for employment, transfer, or remove personnel authorized to have direct access to the system; and
(6) A project may authorize and utilize remote (off-premises) system data bases to the extent that they comply with these security requirements.

(h) All projects shall adopt procedures to assure that all information which is retained by a project has relevancy and importance. Such procedures shall provide for the periodic review of information and the destruction of any information which is misleading, obsolete or otherwise unreliable and shall require that any recipient agencies be advised of such changes which involve errors or corrections. All information retained as a result of this review must reflect the name of the reviewer, date of review and explanation of decision to retain. Information retained in the system must be reviewed and validated for continuing compliance with system submission criteria before the expiration of its retention period, which in no event shall be longer than five (5) years.

(i) If funds awarded under the Act are used to support the operation of an intelligence system, then:

(1) No project shall make direct remote terminal access to intelligence information available to system participants, except as specifically approved by the Office of Justice Programs (OJP) based on a determination that the system has adequate policies and procedures in place to insure that it is accessible only to authorized systems users; and

(2) A project shall undertake no major modifications to system design without prior grantor agency approval.

(j) A project shall notify the grantor agency prior to initiation of formal information exchange procedures with any Federal, State, regional, or other information systems not indicated in the grant documents as initially approved at time of award.

(k) A project shall make assurances that there will be no purchase or use in the course of the project of any

electronic, mechanical, or other device for surveillance purposes that is in violation of the provisions of the Electronic Communications Privacy Act of 1986, Public Law 99-508, 18 U.S.C. 2510-2520, 2701-2709 and 3121-3125, or any applicable State statute related to wiretapping and surveillance.

(l) A project shall make assurances that there will be no harassment or interference with any lawful political activities as part of the intelligence operation.

(m) A project shall adopt sanctions for unauthorized access, utilization, or disclosure of information contained in the system.

(n) A participating agency of an interjurisdictional intelligence system must maintain in its agency files information which documents each submission to the system and supports compliance with project entry criteria. Participating agency files supporting system submissions must be made available for reasonable audit and inspection by project representatives. Project representatives will conduct participating agency inspection and audit in such a manner so as to protect the confidentiality and sensitivity of participating agency intelligence records.
(o) The Attorney General or designee may waive, in whole or in part, the applicability of a particular requirement or requirements contained in this part with respect to a criminal intelligence system, or for a class of submitters or users of such system, upon a clear and convincing showing that such waiver would enhance the collection, maintenance or dissemination of information in the criminal intelligence system, while ensuring that such system would not be utilized in violation of the privacy and constitutional rights of individuals or any applicable state or federal law.

§ 23.30 Funding guidelines.
The following funding guidelines shall apply to all Crime Control Act funded discretionary assistance awards and Bureau of Justice Assistance (BJA) formula grant program subgrants, a purpose of which is to support the operation of an intelligence system. Intelligence systems shall only be funded where a grantee/subgrantee agrees to adhere to the principles set forth above and the project meets the following criteria:

(a) The proposed collection and exchange of criminal intelligence information has been coordinated with and will support ongoing or proposed investigatory or prosecutorial activities relating to specific areas of criminal activity.

(b) The areas of criminal activity for which intelligence information is to be utilized represent a significant and recognized threat to the population and:

(1) Are either undertaken for the purpose of seeking illegal power or profits or pose a threat to the life and property of citizens; and

(2) Involve a significant degree of permanent criminal organization; or

(3) Are not limited to one jurisdiction.

(c) The head of a government agency or an individual with general policy making authority who has been expressly delegated such control and supervision by the head of the agency will retain control and supervision of information collection and dissemination for the criminal intelligence system. This official shall certify in writing that he or she takes full responsibility and will be accountable for the information maintained by and disseminated from the system and that the operation of the system will be in compliance with the principles set forth in § 23.20.

(d) Where the system is an interjurisdictional criminal intelligence system, the governmental agency which exercises control and supervision over the operation of the system shall require that the head of that agency or an individual with general policymaking authority who has been expressly delegated such control and supervision by the head of the agency:

(1) assume official responsibility and accountability for actions taken in the name of the joint entity, and

(2) certify in writing that the official takes full responsibility and will be accountable for insuring that the information transmitted to the interjurisdictional system or to participating agencies will be in compliance with

the principles set forth in § 23.20.

The principles set forth in § 23.20 shall be made part of the by-laws or operating procedures for that system. Each participating agency, as a condition of participation, must accept in writing those principles which govern the submission, maintenance and dissemination of information included as part of the interjurisdictional system.

(e) Intelligence information will be collected, maintained and disseminated primarily for State and local law enforcement efforts, including efforts involving Federal participation.

§ 23.40 Monitoring and auditing of grants for the funding of intelligence systems.
(a) Awards for the funding of intelligence systems will receive specialized monitoring and audit in accordance with a plan designed to insure compliance with operating principles as set forth in § 23.20. The plan shall be approved prior to award of funds.
(b) All such awards shall be subject to a special condition requiring compliance with the principles set forth in § 23.20.

(c) An annual notice will be published by OJP which will indicate the existence and the objective of all systems for the continuing interjurisdictional exchange of criminal intelligence information which are subject to the 28 CFR Part 23 Criminal Intelligence Systems Policies.

Laurie Robinson
Acting Assistant Attorney General
Office of Justice Programs
(FR Doc. 93-22614 Filed 9-15-93; 8:45 am)

1998 Policy Clarification

AGENCY: Bureau of Justice Assistance (BJA), Office of Justice Programs (OJP), Justice.

ACTION: Clarification of policy.

SUMMARY: The current policy governing the entry of identifying information into criminal intelligence sharing systems requires clarification. This policy clarification is to make clear that the entry of individuals, entities and organizations, and locations that do not otherwise meet the requirements of reasonable suspicion is appropriate when it is done solely for the purposes of criminal identification or is germane to the criminal subject's criminal activity. Further, the definition of "criminal intelligence system" is clarified.

EFFECTIVE DATE: This clarification is effective December 30, 1998.

FOR FURTHER INFORMATION CONTACT: Paul Kendall, General Counsel, Office of Justice Programs, 810 7th Street NW, Washington, DC 20531, (202) 307-6235.

SUPPLEMENTARY INFORMATION: The operation of criminal intelligence information systems is governed by
28 CFR Part 23. This regulation was written to both protect the privacy rights of individuals and to encourage and expedite the exchange of criminal intelligence information between and among law enforcement agencies
of different jurisdictions. Frequent interpretations of the regulation, in the form of policy guidance and correspondence, have been the primary method of ensuring that advances in technology did not hamper its effectiveness.

Comments

The clarification was opened to public comment. Comments expressing unreserved support for the clarification were received from two Regional Intelligence Sharing Systems (RISS) and five states. A comment from the Chairperson of a RISS, relating to the use of identifying information to begin new investigations, has been incorporated. A single negative comment was received, but was not addressed to the subject of this clarification.

Use of Identifying Information

28 CFR 23.3(b)(3) states that criminal intelligence information that can be put into a criminal intelligence sharing system is "information relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and . . . meets criminal intelligence system submission criteria." Further, 28 CFR 23.20(a) states that a system shall only collect information on an individual if "there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity." 28 CFR 23.20(b) extends that limitation to [page 71753] collecting information on groups and corporate entities.

In an effort to protect individuals and organizations from the possible taint of having their names in intelligence systems (as defined at 28 CFR Sec. 23.3(b)(1)), the Office of Justice Programs has previously interpreted this section to allow information to be placed in a system only if that information independently meets the requirements of the regulation. Information that might be vital to identifying potential criminals, such as favored locations and companions, or names of family members, has been excluded from the systems. This policy has hampered the effectiveness of many criminal intelligence sharing systems.

Given the swiftly changing nature of modern technology and the expansion of the size and complexity of criminal organizations, the Bureau of Justice Assistance (BJA) has determined that it is necessary to clarify this element of 28 CFR Part 23. Many criminal intelligence databases are now employing "Comment" or "Modus Operandi" fields whose value would be greatly enhanced by the ability to store more detailed and wide-ranging identifying information. This may include names and limited data about people and organizations that are not suspected of any criminal activity or involvement, but merely aid in the

identification and investigation of a criminal suspect who independently satisfies the reasonable suspicion standard.

Therefore, BJA issues the following clarification to the rules applying to the use of identifying information. Information that is relevant to the identification of a criminal suspect or to the criminal activity in which the suspect is engaged may be placed in a criminal intelligence database, provided that (1) appropriate disclaimers accompany the information noting that is strictly identifying information, carrying no criminal connotations; (2) identifying information may not be used as an independent basis to meet the requirement of reasonable suspicion of involvement in criminal activity necessary to create a record or file in a criminal intelligence system; and (3) the individual who is the criminal suspect identified by this information otherwise meets all requirements of 28 CFR Part 23. This information may be a searchable field in the intelligence system.

For example: A person reasonably suspected of being a drug dealer is known to conduct his criminal activities at the fictional "Northwest Market." An agency may wish to note this information in a criminal intelligence database, as it may be important to future identification of the suspect. Under the previous interpretation of the regulation, the entry of "Northwest Market" would not be permitted, because there was no reasonable suspicion that the "Northwest Market" was a criminal organization. Given the current clarification of the regulation, this will be permissible, provided that the information regarding the "Northwest Market" was clearly noted to be non-criminal in nature. For example, the data field in which "Northwest Market" was entered could be marked "Non-Criminal Identifying Information," or the words "Northwest Market" could be followed by a parenthetical comment such as "This organization has been entered into the system for identification purposes only - it is not suspected of any criminal activity or involvement." A criminal intelligence system record or file could not be created for "Northwest Market" solely on the basis of information provided, for example, in a comment field on the suspected drug dealer. Independent information would have to be obtained as a basis for the opening of a new criminal intelligence file or record based on reasonable suspicion on "Northwest Market." Further, the fact that other individuals frequent "Northwest Market" would not necessarily establish reasonable suspicion for those other individuals, as it relates to criminal intelligence systems.

The Definition of a "Criminal Intelligence System"

The definition of a "criminal intelligence system" is given in 28 CFR 23.3(b)(1) as the "arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information . . . ." Given the fact that cross-database searching techniques are now common-place, and given the fact that multiple databases may be contained on the same computer system, BJA has determined that this definition needs clarification, specifically to differentiate between criminal intelligence systems and non-intelligence systems.

The comments to the 1993 revision of 28 CFR Part 23 noted that "the term 'intelligence system' is redefined to clarify the fact that historical telephone toll files, analytical information, and work products that are not either retained, stored, or exchanged and criminal history record information or identification (fingerprint) systems
are excluded from the definition, and hence are not covered by the regulation . . . ." 58 FR 48448-48449 (Sept. 16, 1993.) The comments further noted that materials that "may assist an agency to produce investigative or other information for an intelligence system . . ." do not necessarily fall under the regulation. Id.

The above rationale for the exclusion of non-intelligence information sources from the definition of "criminal intelligence system," suggests now that, given the availability of more modern non-intelligence information sources such as the Internet, newspapers, motor vehicle administration records, and other public record information on-line, such sources shall not be considered part of criminal intelligence systems, and shall not be covered by this regulation, even if criminal intelligence systems access such sources during searches on criminal suspects. Therefore, criminal intelligence systems may conduct searches across the spectrum of non-intelligence systems without those systems being brought under 28 CFR Part 23. There is also no limitation on such non-intelligence information being stored on the same computer system as criminal intelligence information, provided that sufficient precautions are in place to separate the two types of information and to make it clear to operators and users of the information that two different types of information are being accessed.

Such precautions should be consistent with the above clarification of the rule governing the use of identifying information. This could be accomplished, for example, through the use of multiple windows, differing colors of data or clear labeling of the nature of information displayed.

Additional guidelines will be issued to provide details of the above clarifications as needed.

Dated: December 22, 1998.

Nancy Gist
Director, Bureau of Justice Assistance
[FR Doc. 98-34547 Filed 12-29-98; 8:45 am]
BILLING CODE 4410-18-P

EXHIBIT H

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

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

AFFIDAVIT OF DIRECTOR MICHAEL RALLINGS

STATE OF TENNESSEE

COUNTY OF SHELBY

SWORN AFFIDAVIT OF MICHAEL RALLINGS

1. My name is Michael Rallings. I am an adult resident citizen of Shelby County, Tennessee. I am over the age of 21, and I am competent to testify in this matter.

2. The facts in this affidavit are based on my personal knowledge.

3. I am the Director of the Memphis Police Department ("MPD")

4. I was commissioned as a Memphis Police Officer in 1990. I have been employed with the City of Memphis Police Department for approximately 29 years.

5. In 2016, I was appointed interim director of MPD, and then permanent director approximately 6 months later.

6. As Director of MPD, I am responsible for providing public safety to the city of Memphis.

7. I am also responsible for over 2,000 officers in my charge.

8. MPD has worked closely with state, local, and federal agencies to provide safety to the region for decades.

9. Regarding federal agencies, MPD works with the Federal Bureau of Investigation ("FBI"), Department of Justice ("DOJ"), Joint Terrorism Task Force ("JTTF"), and the Drug Enforcement Agency ("DEA"), among others, on a regular basis.

10. MPD also routinely receives intelligence from the Tennessee Fusion Center, as well as other states' law enforcement agencies.

11. Memphis is home to a JTTF, which is an ongoing joint operation between MPD, FBI, Shelby County Sheriff's Department, the Department of Homeland Security, Immigration and Customs Enforcement, and the Transportation Security Administration. The JTTF allows these law enforcement agencies to share intelligence seamlessly and to cooperate with each other more effectively.

12. If MPD cannot share and receive information freely with these federal law enforcement agencies, that will effectively end MPD's participation in the JTTF.

13. If MPD is not able to participate in the JTTF, or is unable to receive intelligence from the Tennessee Fusion Center, FBI, Department of Homeland Security, Shelby County Sherriff's Department, and other states' law enforcement agencies, the safety of the greater Memphis region will be at risk.

14. MPD also participates in the Multi-Agency Gang Unit ("MGU"). The MGU was formed in 2011, and is a group of elite members of MPD, Shelby County Sheriff's Office Narcotics Division, ATF, FBI, and the U.S. Marshals. MGU's purpose is to conduct long term investigations

on criminal gangs and to dismantle gang organizations

15. MGU has been very successful at fighting gangs in Memphis. In June 2019, a federal jury found five members of the Conservative Vice Lords Concrete Cartel criminal gang guilty of conspiracy to participate in racketeering activities, multiple armed pharmacy robberies, and drug trafficking conspiracy.

16. One of the defendants was a Tennessee statewide gang leader and another was a citywide gang leader. The remaining defendants were branch leaders in the organization, claiming areas in East Memphis, Orange Mound, and Whitehaven. This federal prosecution and guilty verdict was the result of an extensive investigation which began in 2015 by FBI's Safe Streets Task Force and the MGU.

17. MGU has been instrumental in the implementation of several "gang injunctions." In September 2013, as the direct result of MGU investigations into reports of criminal gang activity in the Riverside area of South Memphis, the Shelby County District Attorney's Office filed the first nuisance petition against the "Riverside Rollin' 90's Neighborhood Crips" ("R90"). In response to the petition, General Sessions Court Judge Larry Potter issued an injunction against R90 members, creating a 4.6-square-mile "safety zone."

18. This process was followed three more times to obtain five more injunctions: (1) October 2014 against the "Dixie Homes Murda Gang/47 NHC" ("DHMG") in the North Main precinct; (2) December 2014 for two injunctions against the "FAM Mob" in two areas of the Old Allen precinct; and (3) January 2016 for injunctions against the "Grape Street Crips" (GSC) and "Vice Lords" (VL) in two overlapping areas of the Tillman Precinct.

19. In each instance, the gang was declared a "public nuisance," and members were required to abide by eleven requirements with respect to their behaviors in the safety zones, including that gang members are not permitted to associate with one another in public, other than

while attending school or church.

20. . Without MPD's participation in the MGU, the MGU will no longer be able to function in the same manner due to the volume of MPD officers in the unit.

21. MPD also greatly relies on the intelligence it receives from the CrimeStoppers program. CrimeStoppers provides tipsters an avenue for their anonymous tips regarding unsolved felony crimes and fugitives wanted.

22. Without the tips from CrimeStoppers, it would be much more difficult for MPD to solve crime.

23. In fact, tips from CrimeStoppers have resulted in over 200 felony arrests in 2019 alone, resolving at least 135 cases. Without the intelligence from CrimeStoppers, these 135 cases would likely not be solved.

24. MPD also actively shares information and intelligence with the Shelby County Sherriff's Department which operates within the Shelby County Schools system.

25. The Shelby County Sheriff's Department provides security via its deputies within several local schools. Shelby County Sherriff's deputies often receive intelligence from students of potential gatherings that are planned that could end in violence.

26. MPD also receives anonymous tips from Shelby County Schools vis the Safe School Tips program. This service allows any parent, student, or employee to report information about illegal or inappropriate activities via text message anonymously anytime someone has a safety concern for herself or other students.

27. MPD also participates with Shelby County and CrimeStoppers in a program called "Trust Pays." Trust Pays offers a safe way for students to confidentially inform a school administrator of a serious incident and potentially receive a cash reward as a result.

28. If MPD is unable to receive and act on the intelligence received the Trust Pays

Program, the Safe School Tips Program, and from the Shelby County Deputies placed within the Shelby County Schools System, the safety of Memphis schoolchildren will be at greater risk.

FURTHER AFFIANT SAITH NOT.

MICHAEL RALLINGS

SUBSCRIBED AND SWORN TO before me on this the 25th day of September, 2019.

Notary Public

PAMELA PATTERSON
STATE OF TENNESSEE NOTARY PUBLIC
SHELBY COUNTY
MY COMMISSION EXPIRES 4-26-2020

My Commission Expires:
April 26, 2020

EXHIBIT I

PUBLIC SAFETY INSTITUTE SPRING 2019

Interim Assessment of Gang Injunctions and Safety Zones in Memphis

Dr. Angela Madden
Research Associate Professor

Mapping by Dr. James McCutcheon
Department of Criminology and Criminal Justice

TABLE OF CONTENTS

MESSAGE FROM THE EXECUTIVE DIRECTOR

Under a funding agreement between the University of Memphis Public Safety Institute (PSI) and the Memphis Shelby Crime Commission, the PSI is charged with assessing and evaluating various objectives under the local Operation: Safe Community plan to reduce and prevent crime.

A key objective of the Operation: Safe Community plan is enhanced information gathering and other resources to reduce gang-related violence. One of the key steps being taken by the Memphis Police Department and the District Attorney's Office is use of enhanced information gathering to seek court injunctions requiring specified members of particular gangs to abide by certain conditions in certain geographic areas called "safety zones."

This research interim assessment is designed to look at the effectiveness of safety zone injunctions. This assessment seeks to address three research questions:

(1) Do injunctions reduce the number of violent offenses in the safety zone areas?
(2) Do gang injunctions reduce arrests of individuals subject to the injunctions?
(3) Do police officers working in precincts with safety zones know about the injunctions and prohibited behaviors?

There are clear limitations on this interim assessment. The PSI plans to conduct a more thorough evaluation at a later date.

Many thanks to Dr. Angela Madden, PSI research associate professor, for her in-depth research on this assessment and to Dr. James McCutcheon for his assistance in the mapping on the assessment.

Bill Gibbons, Executive Director
Public Safety Institute

INTRODUCTION

In Sept. 2013, as the result of Multi-Agency Gang Unit (MGU) investigations into reports of criminal gang activity in the Riverside area of South Memphis (part of the Memphis Police Department's Airways precinct), the Shelby County District Attorney's Office (DA) filed the first nuisance petition against the "Riverside Rollin' 90's Neighborhood Crips" (R90). In response to the petition, General Sessions Court Judge Larry Potter issued an injunction against R90 members, creating a 4.6-square-mile "safety zone." This process was followed three more times to obtain five more injunctions: 1) Oct. 2014 against the "Dixie Homes Murda Gang/47 NHC" (DHMG) in the North Main precinct; 2) Dec. 2014 for two injunctions against the "FAM Mob" in two areas of the Old Allen precinct and 3) Jan. 2016 for injunctions against the "Grape Street Crips" (GSC) and "Vice Lords" (VL) in two overlapping areas of the Tillman Precinct.

In each instance, the gang was declared a "public nuisance," and members were required to abide by the following 11 requirements with respect to their behaviors in the safety zones:

1. Do not associate | Members may not appear together in public view or any place accessible to the public (does not include inside a school while attending classes or a place of worship).

2. No intimidation | Members may not confront or provoke any person known to be a witness to any activity of gang members.

3. No guns or dangerous weapons | Members may not possess any gun ammunition or illegal weapons, and must not remain in the presence of them.

4. No graffiti or graffiti tools | Members may not damage or deface private property of others or possess tools for the purpose of "tagging" private property of others.

5. Stay away from drugs | Members may not possess, sell or use any controlled substance or paraphernalia without a prescription.

6. Do not act as a lookout | Members may not act as lookouts to warn of the approach or presence of law enforcement.

7. Stay away from alcohol | Members may not possess any open alcohol container while in public view or in any public place.

8. No trespassing | Members may not be present on or in any private property not open to the public without owner consent.

9. No forcible recruiting | Members may not make threats to strike or assault another person nor damage or destroy personal property or disturb the peace to encourage a person to join the gang.

10. No preventing a member from leaving the gang | Members may not make threats to strike or assault another person nor damage or destroy personal property to prevent a person from leaving the gang.

11. Obey all laws.

The injunctions give law enforcement the authority to arrest any gang member found in violation of these court-ordered conditions. Police may arrest violators and charge them with contempt of court. However, violating gang members subject to injunction must previously have been served notice (i.e., informed that they are subject to the injunction) by Shelby County deputy sheriffs before they can be arrested and charged under the injunction. In addition, an individual can "opt out" of the injunctions by providing a 30-day notice to the DA, providing a written declaration that he or she was not or is no longer a member of the gang and by providing proof of that non-association. To date, one individual originally included in the FAM Mob injunction has successfully opted out.

While anecdotal evidence may suggest that these injunctions are effective in curtailing gang activity and reducing violent crime in Memphis, no systematic investigation into their impact previously had been conducted. This need was recognized by the Memphis Shelby Crime Commission (MSCC) in developing the third iteration of its *"Operation: Safe Community Crime Plan"* (OSC-3). Goal B of the five-year plan is to "strengthen law enforcement's ability to reduce violent street crime." Within this goal, Objective B4 aims to reduce gang violence through enhanced intelligence and data-gathering. The process of filing a petition for an injunction is driven by street-level intelligence and data that must be assembled to support the need for an injunction. A finding that injunctions are indeed effective at reducing gang violence would provide evidence that Objective B4 is being attained. In addition, gathering and analyzing data to measure whether injunctions are effective can inform and enhance law enforcement and prosecutorial strategies to address gang violence.

While the University of Memphis Public Safety Institute (PSI) plans to conduct a full pre-/post-implementation evaluation at a later date, this interim report provides some insight into violent crime and gang member behavior since injunctions were implemented. Moreover, this process sets up the templates that will be required for a full evaluation.

LITERATURE REVIEW

What is a Gang?

No universally accepted definition of "gang" exists, so jurisdictions usually develop their own. The image most commonly associated with a gang is that of the "street gang." This term often is interchanged with "youth gang" and "criminal street gang," although the latter is characterized by criminal activity of specific interest to local, state and federal gang-related legislation. The term "street gang," however, may be most instructive because it implies crimes committed by a group with a street presence, which is a key characteristic of youth gangs. Most importantly, the acts committed by these groups often are serious violent crimes that take place on community streets, such as aggravated assaults, drive-by shootings, robberies, car-jackings and homicides. Citizens and policymakers are especially concerned about these offenses because their perpetration increases resident fear and significantly impacts the community's ability to effectively implement mechanisms of informal social control (National Gang Center, 2019).

Jurisdictions often use the following criteria to classify groups as gangs:

- The group has three or more members, generally aged 12–24.
- Members share an identity, typically linked to a name and often other symbols.
- Members view themselves as a gang and are recognized by others as a gang.
- The group has some permanence and a degree of organization.
- The group is involved in an elevated level of criminal activity.

Currently, federal law (18 U.S.C. § 521) defines a "criminal street gang" as an "ongoing association of five or more persons that has as one of its primary purposes the commission of federal felonies involving controlled substances for which the maximum penalty is not less than five years, federal felony crimes of violence and conspiracies to commit such offenses, whose members have engaged in a continuing series of such offenses within the past five years and such activities affect interstate or foreign commerce."

This federal definition differs markedly from other definitions because the federal system is more concerned with large-scale criminal enterprises that cross state or national boundaries. At the state and local level, results from the National Youth Gang Survey (NYGS), conducted by the National Gang Center (NGC) from 1996 through 2012, indicate that law enforcement agencies believe a group name, group identity, criminal activity and using symbols and signs to represent the group to others to be the most important characteristics of defining a group as a gang (National Gang Center, 2019).

What is a Gang Member?

The definition of a "gang member" is also inconsistent across jurisdictions, with common definitional points being admission of gang involvement, being identified as a gang member by a reliable witness (often a parent or guardian) and having identifiable symbols associated with the gang such as clothing or tattoos (National Gang Center, 2019). Developing a solid operational definition for the term "gang member" is crucial for communities to identify these individuals, to develop effective strategies to deal with them and for prosecution efforts.

Federal law (18 U.S.C. § 521) considers a gang member to be any person who:

(1) Participates in a criminal street gang with knowledge that its members engage in or have engaged in a continuing series of [gang] offenses.

(2) Intends to promote or further the felonious activities of the criminal street gang or maintain or increase his or her position in the gang.

(3) Has been convicted within the past five years for:

(A) A federally defined gang offense.

(B) A state offense:

(i) Involving a controlled substance (as defined in section 102 of the Controlled Substances Act [21 USC § 802]) for which the maximum penalty is not less than five years' imprisonment; or

(ii) that is a felony crime of violence that has as an element the use or attempted use of physical force against the person of another.

(C) Any federal or state felony offense that by its nature involves a substantial risk that physical force against the person of another may be used in the course of committing the offense.

(D) A conspiracy to commit an offense described in subparagraph (A), (B) or (C).

Several states and local jurisdictions require an individual to meet certain criteria and/or thresholds to be classified as a gang member. Many states require that multiple criteria be met, such as the identification of the person as a gang member by a reliable source and the outward display of gang symbols, hand signs and/or gang tattoos by the individual in question (Tita & Papachristos, 2009).

What is a Gang Crime?

Definitions of gang crime also vary between jurisdictions. These definitions range from wholly encapsulating statements regarding crimes committed with the knowledge that the crime was being committed as part of a gang or with others known to be in a gang, to more specific lists of violations and offenses considered gang crimes (e.g., acts involving controlled substances or deadly weapons, assault, burglary and arson). Many state definitions specify that the crime must have been committed with the knowledge that the crime may further the individual's standing in a gang or that the activity can be identified as gang activity by a reliable witness (National Gang Center, 2016).

Many jurisdictions encounter difficulty in determining when to classify a criminal act involving a gang member, or potential gang member, as a "gang crime." Jurisdictions use the terms "gang-involved," "gang-related," and/or "gang-motivated" and often erroneously use these terms interchangeably when they should be distinct.

Most distinctions relate to the intent or motive of the offender and in determining which criminal acts are related to his or her status as a gang member. Clearly, crime committed by a gang member that is irrelevant to his or her status as a gang member should not be considered gang crime in the strictest sense. Some jurisdictions, however, call these types of crimes "gang-involved" or "gang-related" simply because they are committed by a gang member.

Acts that are committed with an intent or motive directly related to the offender's gang membership, or potential gang membership, often are termed "gang-motivated." These are the types of offenses about which jurisdictions are most concerned. Gang-motivated crime is directly linked to gang membership and comprises most reported gang crime. These types of crimes include violence between rival gangs or crimes committed on behalf of the gang (Rosenfeld, Bray & Agley, 1999).

Determining intent, motive and whether an act is simply committed by a gang member or is committed by a gang member for gang purposes can be problematic. Domestic assault, for example, may be committed by a gang member and be classified as simply gang-involved or gang-related because the offender is a gang member. When the assault, however, is encouraged by fellow gang members or is used by the offender to attain status in the gang, it becomes gang-motivated. The definitions regarding gangs and gang violence must be considered in relevant policies, which may impact the criminal justice proceedings dealing with gang members.

Gangs, Gang Members and Gang Crimes in Tennessee

Tennessee law (T.C.A. 40-35-121) defines a "criminal gang" as a "formal or informal ongoing organization, association or group consisting of three or more persons that has:

(A) As one of its primary activities, the commission of ***criminal gang offenses;***

(B) Two or more members who, individually or collectively, engage in or have engaged in a ***pattern of criminal gang activity***.

The statute outlined a limited number of ***criminal gang offenses*** prior to July 1, 2013. However, beginning on July 1, 2013, the scope was broadened to include the "commission of or attempted commission of, facilitation of, solicitation of, or conspiracy to commit" a list of 27 criminal offenses, from murder, rape and kidnapping, to witness coercion, retaliation and inciting to riot.

Also important to the Tennessee statute is a ***"pattern of criminal gang activity."*** To constitute a pattern, the individuals in questions must have "prior convictions for the commission of or attempted commission of, facilitation of, solicitation of or conspiracy to commit:

(i) Two or more criminal gang offenses that are classified as felonies.

(ii) Three or more criminal gang offenses that are classified as misdemeanors.

(iii) One or more criminal gang offenses that are classified as felonies and two or more criminal gang offenses that are classified as misdemeanors.

(iv) The criminal gang offenses are committed on separate occasions.

(v) The criminal gang offenses are committed within a five-year period.

Tennessee is one of several states that has established criteria for defining a "criminal gang member." For an individual to be considered a gang member in Tennessee, he or she must meet at least two of the following criteria:

- Admits to criminal gang involvement.
- Is identified as a criminal gang member by a parent or guardian.
- Is identified as a criminal gang member by a documented reliable informant.
- Resides in or frequents a particular criminal gang's area; adopts its style of dress, use of hand signs or tattoos; and associates with known gang members.
- Is identified as a criminal gang member by an informant of previously untested reliability, and such identification is corroborated by independent information.
- Has been arrested more than once in the company of identified criminal gang members for offenses that are consistent with usual criminal gang activity.
- Is identified as a criminal gang member by physical evidence such as photographs or other documentation.

Programs and Policies to Address Gang Violence

The National Institute of Justice (NIJ) lists 24 programs and one practice that have been developed to address gang violence (crimesolutions.gov). Of the 24 programs, six have been rated as "effective," 13 as "promising" and five as having "no effects." Of the six effective programs, two were focused deterrence programs (Los Angeles and New Orleans), two were problem-oriented, community-policing programs (Operation Ceasefire in Boston, Operation Peacekeeper in Stockton, Calif.), one was a detention-based intervention program (Project BUILD in Chicago) and one was a Los Angeles program based on "crime-prevention through environmental design" (CPTED) principles that installed physical street barriers in some residential areas with high levels of gang violence.

The practice identified by NIJ as focused deterrence rated as "promising."
Focused deterrence strategies:

> Target specific criminal behavior committed by a small number of chronic offenders who are vulnerable to sanctions and punishment. Offenders are directly confronted and informed that continued criminal behavior will not be tolerated. Targeted offenders are also told how the criminal justice system, such as the police and prosecutors, will respond to continued criminal behavior; mainly that all potential sanctions or levers will be applied. The deterrence-based message is reinforced through crackdowns on offenders, or groups of offenders, such as gang members, who continue to commit crimes despite the warning. In addition to deterring violent behavior, the strategies also reward compliance and nonviolent behavior among targeted offenders by providing positive incentives, such as access to social services and job opportunities.

Although two of the effective programs used focused deterrence and these strategies are deemed "promising," two of the five programs with "no effects" also were based on principles of focused deterrence (Group Violence Reduction Strategy in Chicago and No Violence Alliance in Kansas City, Mo.).

In addition to programs and practices, jurisdictions plagued by gang violence also have legal tools at their disposal. Civil gang injunctions (CGI), for example, are a type of restraining order issued by courts to prohibit gang members in specific areas from participating in specific activities. They are based on the legal theory that gang activities create a public nuisance that prevents other community members from having public order and peace. Usually, injunctions are obtained against the gang as a unit. However, police and prosecutors later identify specific gang members who are subject to the injunction.

The Los Angeles city attorney and the Los Angeles Police Department (LAPD) obtained the first CGI against gangs on July 22, 1982, specifically to address gang graffiti (Simpson, 2013). Since then, cities in California have been the primary users of this tool. Throughout the 1980s and into the mid-2010s, hundreds of CGIs covering tens of thousands of individuals were obtained in several California cities based primarily on anecdotal evidence of their effectiveness.

A few studies have attempted to measure the impact of CGI on gang activities. One study evaluated 25 gang injunctions from four California counties matched with similar communities with similar gang problems but no injunctions. Researchers evaluated calls for service during the year before the injunction and the year after the injunction. Calls for service in the injunction areas significantly decreased over the baseline and compared to the matched communities. The authors concluded that gang injunctions, implemented correctly, can reduce gang crime (O'Deane & Morreale, 2011).

A more recent and comprehensive study from Los Angeles examined the impact of 46 injunctions enacted from 1993 through 2013 (Ridgeway, Grogger, Moyer & MacDonald, 2018). The researchers compared reported crime in affected geographic areas before and after the injunctions and contrasted those data with data from areas not covered by injunctions. This allowed them to examine the average short- and long-term impact. They concluded that injunctions seemed to reduce crime by about five percent in the short-term and by as much as 18 percent in the long-term. The reduction in assaults was much larger, about 19 percent in the short-term and 35 percent in the long-term. The authors also found no evidence that the injunctions displaced crime to nearby areas.

Other research indicates that positive results may be short-lived. A study of five San Bernardino neighborhoods found that while most of the neighborhoods had less crime and gang presence immediately following the injunctions, the reduction was short-lived. Moreover, one of the neighborhoods experienced increased gang activity after the injunction (Maxson, Hennigan & Sloane, 2005).

Gang injunctions are not without their critics. Numerous lawsuits have challenged their constitutionality (i.e., freedom of assembly, due process). Other criticisms include those related to the suppression effect which may diminish alternatives and diversion programs for at-risk youth, their zero-tolerance nature, which may punish even benign activities of two gang members and their disproportionate impact on youth of color.

In 2016, the American Civil Liberties Union (ACLU) filed suit against the city of Los Angeles, arguing that the filing of an injunction against a gang, rather than against an individual, denied an individual the opportunity to disprove his or her alleged gang affiliation in court. Following this suit, the Los Angeles city attorney and the LAPD conducted an audit of the injunction rolls to determine which individuals could be removed due to no longer posing a threat, being deceased, having relocated, etc. This resulted in the purging of some 7,300 people from the injunction lists in 2017. Most recently, a federal judge prohibited the LAPD from enforcing existing injunctions against anyone who did not have the opportunity to challenge the "gang member" designation in court before being subject to the injunction, (Winter & Queally, 2018).

METHODS

Two primary research questions are addressed with this interim report and will be addressed with the full evaluation. The main difference is that the full evaluation will compare pre-injunction data (beginning Jan. 1, 2010) to post-injunction data (through 2021) while this report examines primarily post-injunction data since Jan. 1, 2014. The research questions addressed are:

1) Do injunctions reduce the number of violent offenses in injunction areas? (Is there a general deterrent effect?)

2) Do gang injunctions reduce arrests of individuals subject to injunctions? (Is there a specific deterrent effect?)

Data required to answer these questions includes: the number of violent offenses within safety zones since issuance of injunctions, and injunction violations and/or number of arrests of gang members since enjoined. Violent offenses are murder, aggravated assault, robbery and rape. Although violent offenses are the focus, the research also considers non-violent offenses involving guns, such as misdemeanor and felony weapons violations.

A third question is addressed because of its implications for law enforcement actions in the safety zones. Do officers working in precincts that have safety zones know about the injunctions and the prohibited behaviors? If officers are unaware of safety zones and prohibited behaviors, they cannot enforce those injunctions and any observed changes in violent offenses or arrests cannot necessarily be attributed to the injunctions. Data required to answer this question included the percentages of correct responses to a questionnaire about safety zones and prohibited behaviors that were distributed to all MPD precincts and completed during roll calls.

Measuring Violent Offenses

To determine the number of violent offenses within safety zones, those zones had to be defined within a "Geographic Information Systems" (GIS) mapping program (i.e., ArcGIS). The MGU provided the PSI with the safety zone boundaries that were used to create "shape files" of the zones. These shape files were overlaid on city maps to circumscribe the boundaries for subsequent data inquiry. Once the geographic boundaries of the safety zones were plotted on maps of the city, the locations of violent offenses from Jan. 2014 through June 2018 were plotted on those maps using MPD offense data. Figures 1–5 provide examples with plots of violent offenses within each safety zone from Jan.–June 2018 only.

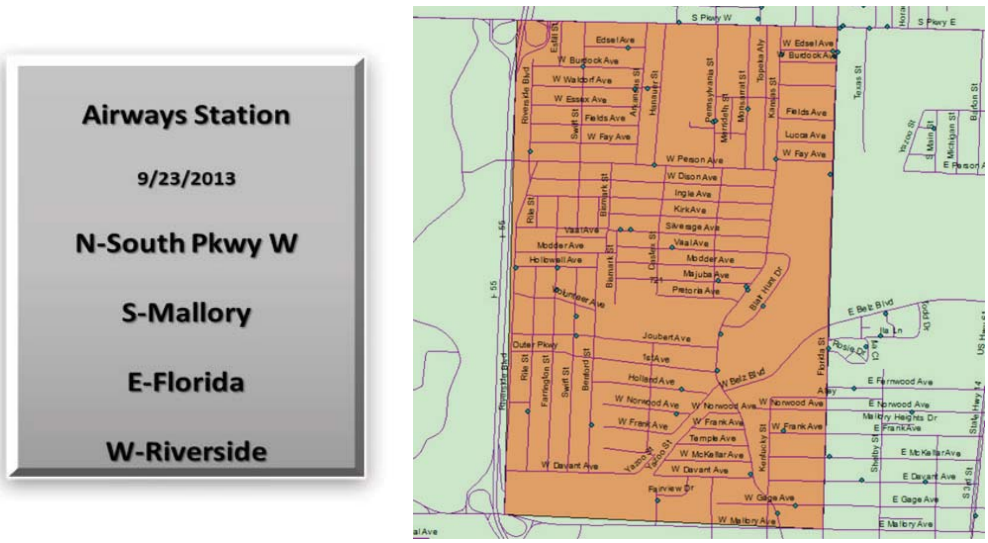

Figure 1: *Airways Station (Rollin' 90s) Safety Zone Violent Offenses (Jan.–June 2018)*

Figure 2: *North Main Station (DHMG/47NHC) Safety Zone Violent Offenses (Jan.–June 2018)*

Figure 3: *Old Allen Station Safety Zone (Greenbriar-FAM Mob) Violent Offenses (Jan.–June 2018)*

Figure 4: *Old Allen Station Safety Zone (Ridgecrest-FAM Mob) Violent Offenses (Jan.–June 2018)*

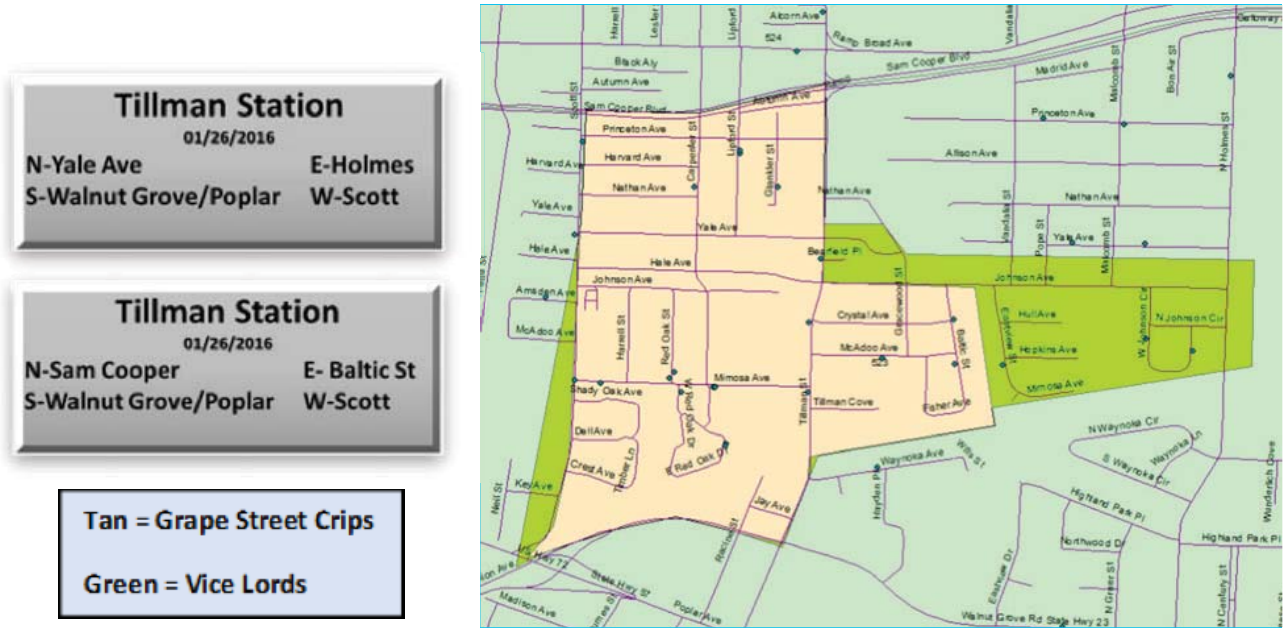

Figure 5: *Old Allen Station Safety Zone (Greenbriar-FAM Mob) Violent Offenses (Jan.–June 2018)*

In addition to maps, line graphs depicting six-month totals of violent offenses from Jan. 1, 2014, through June 30, 2018, in all the zones, as well as by zone, were produced. Although it is desirable to plot data over more points in time (i.e., monthly), the number of violent offenses each month in some of the zones would have been too low to make the graphs meaningful. Trends over time with respect to injunction dates in each zone were observed and any changes noted.

Measuring Arrests of Enjoined Individuals

A total of 120 individuals currently are covered under the injunctions: 26 in Rollin' 90's, 34 in DHMG/47NHC, 28 in FAM Mob, 13 in Grape Street Crips and 19 in Vice Lords. The Shelby County gang injunctions were designed to impact the gang behavior of those 120 people in six well-defined small areas. That gang behavior could be simply associating with another gang member or it could be committing an aggravated assault. In addition to examining arrests related to the safety zones, it was also important to collect and analyze data about arrests of those individuals outside the safety zones. If gang injunctions reduce arrests beyond the safety zones, they have a more significant impact on crime than originally intended. Therefore, determining the extent to which enjoined individuals were arrested required the collection and analysis of data from several different sources, including the DA (arrests and prosecutions for injunction violations), the MGU (monthly reports of gang members arrested for gun crime) and the MPD (citywide arrests for violent crime and gun crime).

The DA and City Attorney's Office compiled and provided the PSI data on enjoined individuals and those arrested and charged since Sept. 2013 under TCA 29-3-111, the statute that proscribes the penalty for violating an order to abate. This provides a measure of injunction violations. In addition, the MGU provided the PSI with monthly lists of gang members arrested for gun crime since April 2018, when they started keeping that data. Finally, the PSI maintains a database of citywide arrests for violent crime, violent gun crime and any gun crime (including misdemeanor and felony weapons violations). The full evaluation will compare the number of arrests of enjoined individuals for violent crimes during some years prior to the date of their service of notice to the number of arrests they have had in the time since injunction.

Measuring Officer Awareness

MPD officers and command staff at all nine precincts were surveyed with a questionnaire during roll calls over one week. The one-page questionnaire, developed by the PSI and reviewed and approved by the MPD command staff, consists of an introductory paragraph that explains the purpose and provides instructions for responding followed by nine questions to measure awareness and understanding and two demographic questions. A total of 628 completed questionnaires, representing about one-third of sworn MPD personnel, were returned to the PSI with the responding precinct noted (see Figure 6). PSI staff scored each response and entered the data into an Excel spreadsheet which was subsequently transformed for analysis using IBM-Statistical Package for Social Sciences (SPSS). Most respondents were patrol officers, and those with more than 10 years of service comprised the largest group of respondents (see Figure 7).

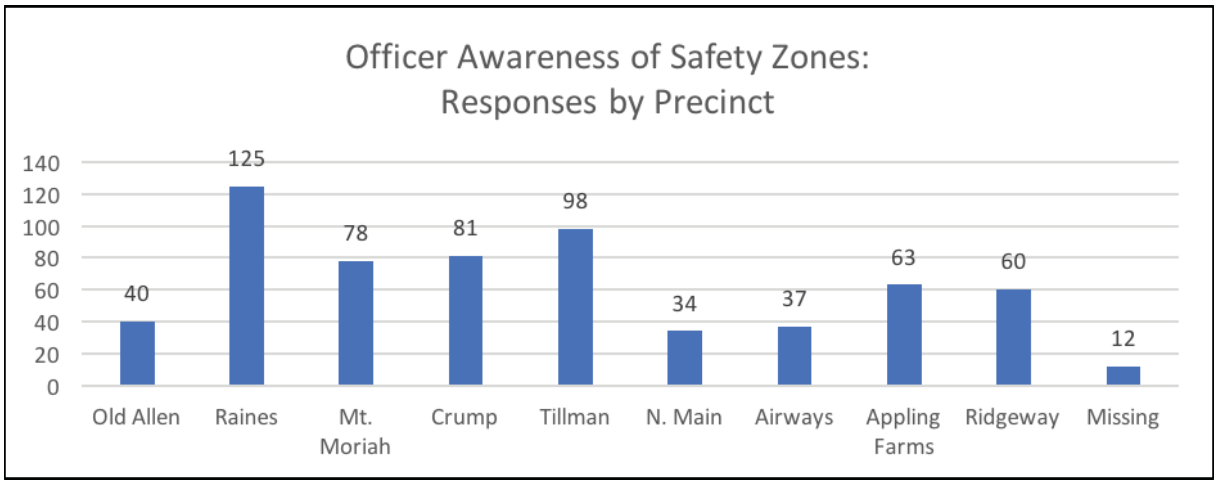

Figure 6: *Officer Awareness of Safety Zones: Responses by Precinct*

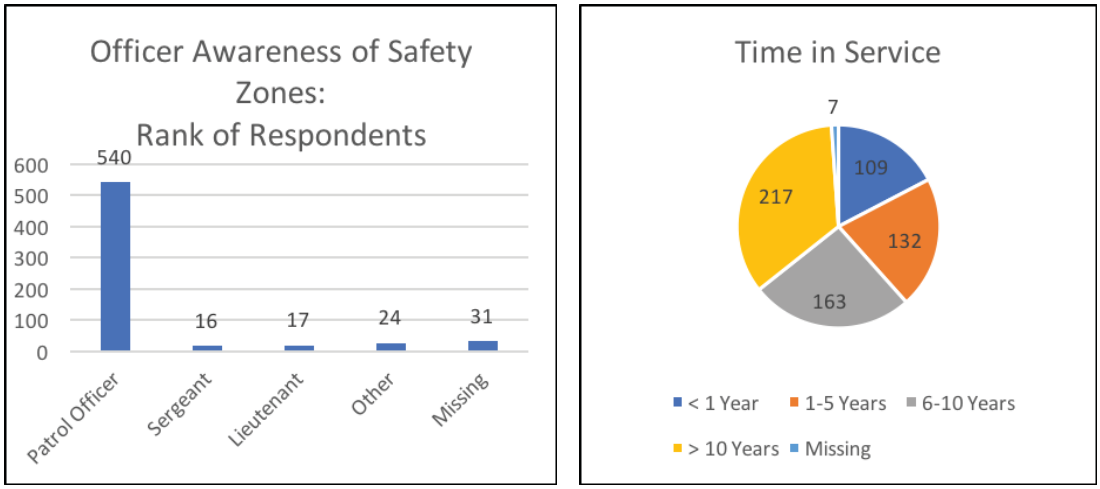

Figure 7: *Officer Awareness of Safety Zones: Rank of Respondents (left) and Time in Service (right)*

ANALYSIS AND RESULTS

Violent Offenses

Measuring the general deterrent effect of the injunctions requires analyzing violent offenses in the safety zones. If all violent offending decreases and not just violent offending by enjoined gang members, the injunctions may have a general deterrent effect. During the period, a total of 1,268 violent offenses were reported in the six safety zones around the city, an average of about one per week per zone. Since Jan. 1, 2014, however, reports have decreased 7.8 percent, from 141 in the first 6 months of 2014 to 130 in the first six months of 2018 (see Figure 8). After an increase of more than 10 percent in the latter half of 2014, numbers have steadily been decreasing as indicated by the dotted blue trendline.

The red vertical lines indicate the six-month periods within which injunctions were issued. This report uses limited data prior to Jan. 2014, but the full evaluation will be able to plot trendlines before the first Sept. 2013 injunction to determine whether trends had been increasing or decreasing before then. Violent offending peaked during the quarter two injunctions were issued and generally have been decreasing since then. The lowest number was in the first half of 2016, during which two injunctions were issued against gangs in the Tillman Precinct.

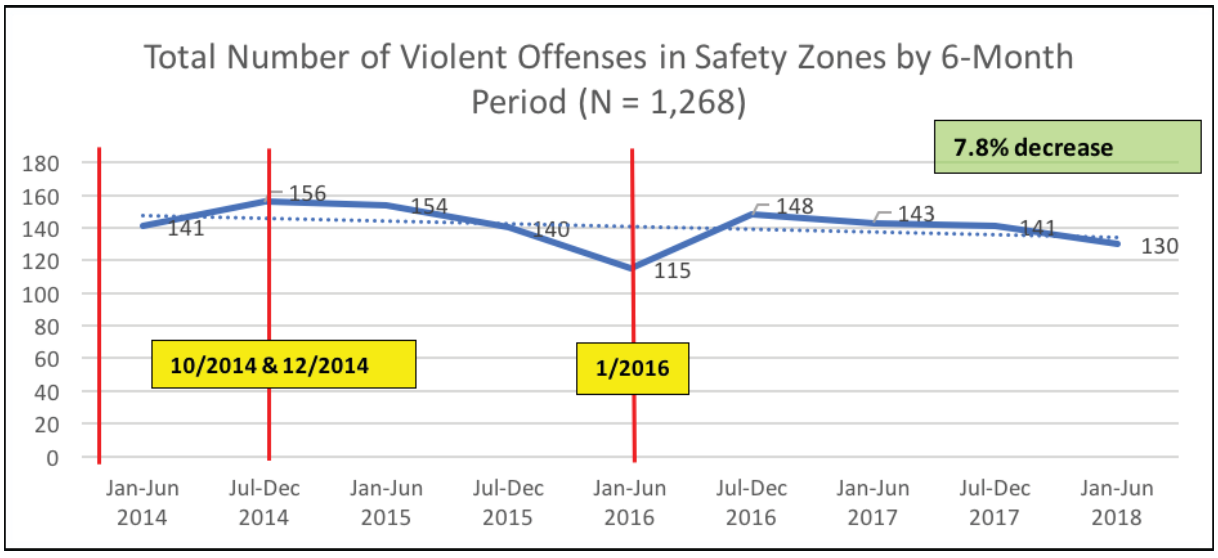

Figure 8: *Total Violent Offenses in Safety Zones by 6-Month Period*

Airways: Created by the first injunction in Sept. 2013, the Airways safety zone had the highest total number of offenses of any single safety zone and averaged more than 1.5 violent offenses per week between Jan. 1, 2014 and June 30, 2018. (see Figure 9). However, this zone also experienced the most dramatic decrease in violent offenses, from 61 in Jan.–June 2014 (an average of about 2.3 per week) to 40 in Jan.–June 2018 (an average of about 1.5 per week), a 34.4 percent decrease in violent offenses. After a steep decline throughout June 2016, numbers increased until beginning a slight decline in July–Dec. 2017. Despite the significant decrease since Jan. 2014, the number of violent offenses in Airways safety zone remains the highest of any zone.

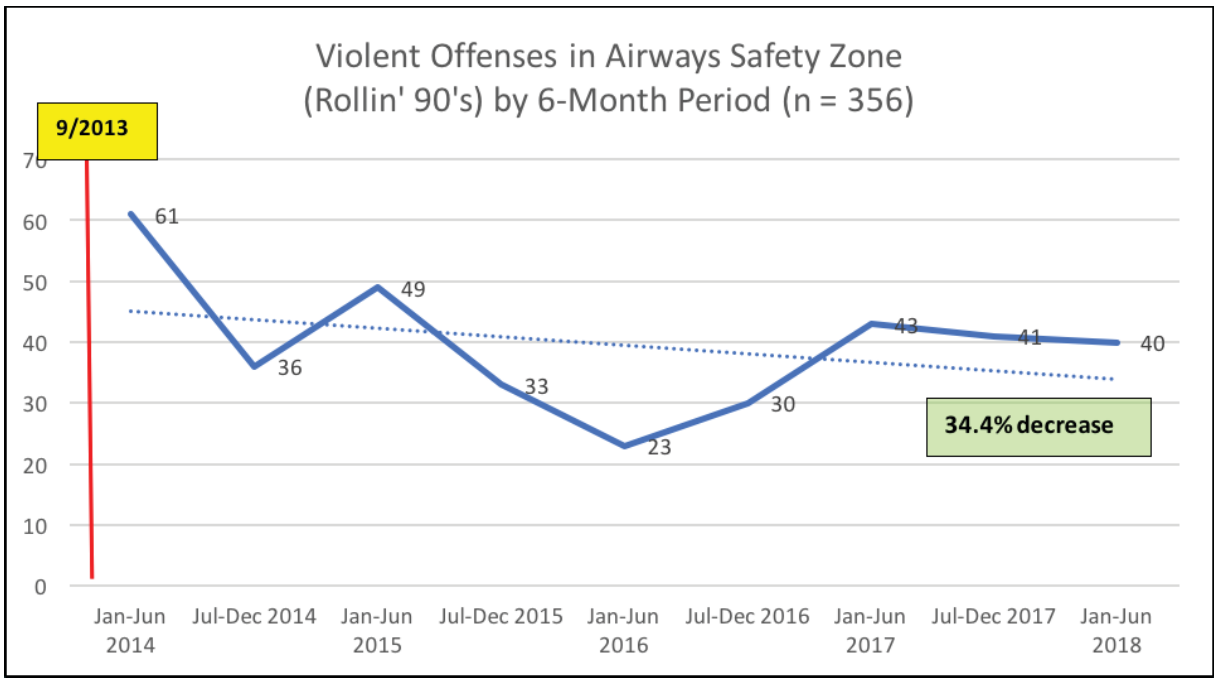

Figure 9: *Violent Offenses in Airways Zone by 6-Month Period*

North Main: The pattern of violent offenses in the North Main safety zone is interesting and illustrates the importance of context (see Figure 10). If the starting point for measuring change is the period Jan.—June 2014, the number of violent offenses *increased* 43.5 percent (from 23 to 33). If the starting point is the period July–Dec. 2014, during which the injunction was issued, the number of violent offenses *decreased* 13.2 percent (from 38 to 33). It is likely that the startling 65 percent increase in violent offenses in this area from the first half of 2014 (n=23) to the next half (n=38) supported the need for an injunction, especially if the 38 offenses during July–Dec. occurred primarily during July, August and September. Although North Main is the smallest precinct, its safety zone had the second highest number of violent offenses during Jan.–June 2018 and averaged more than 1.2 violent offenses per week during the entire period.

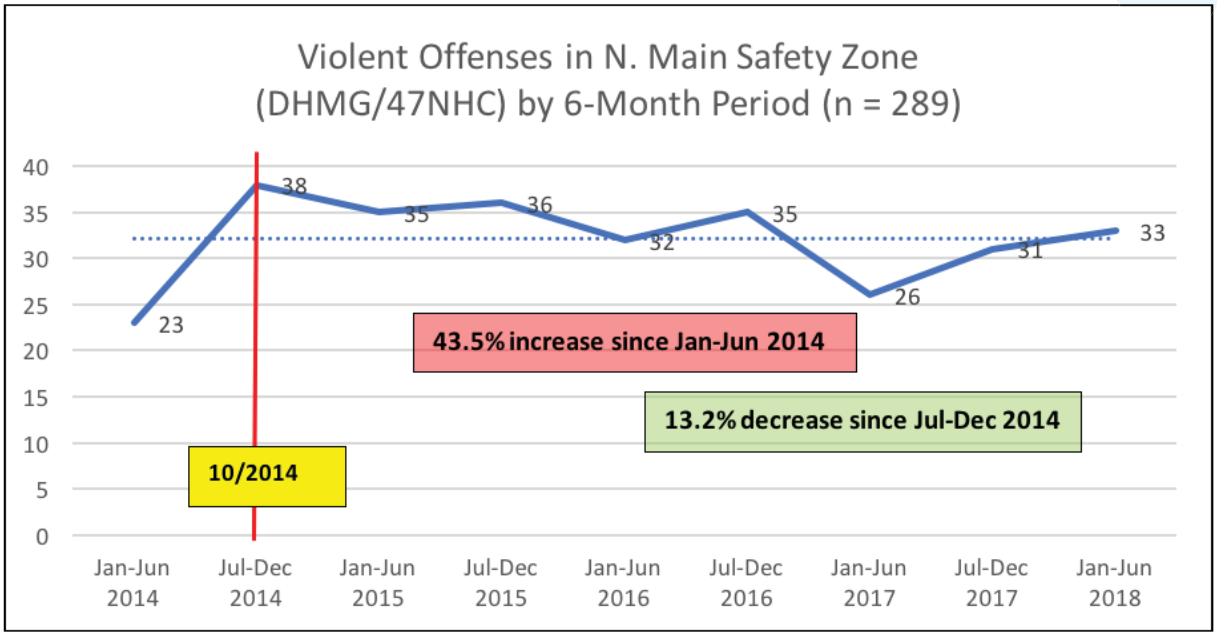

Figure 10: *Violent Offenses in N. Main Zone by 6-Month Period*

Old Allen: Safety zones in Old Allen concentrate on areas surrounding two apartment complexes, Greenbriar and Ridgecrest, (see Figure 11). Violent offenses in both zones combined (n=196) was lower than any other single zone and averaged .84 violent offenses per week. As single zones, Ridgecrest averaged .51 violent offenses per week and Greenbriar averaged .32.

At the beginning of the period, the number of violent offenses in Ridgecrest was nearly 67 percent higher than the number in Greenbriar. However, a 26.7 percent decrease in Ridgecrest has brought their numbers much closer together. In fact, the number of violent offenses in Greenbriar surpassed the number in Ridgecrest during the latter half of 2017. Despite some spikes and dips, the number of violent offenses in Greenbriar at the end of June 2018 was the same as it was during the first half of 2014.

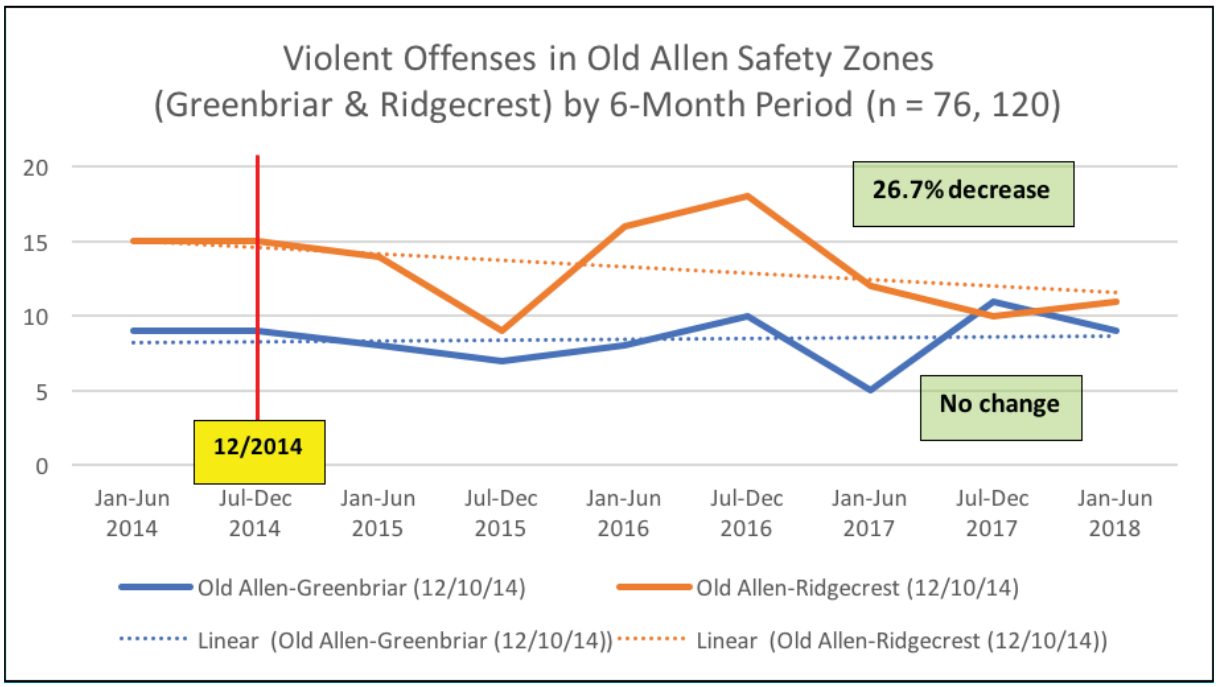

Figure 11: *Violent Offenses in Old Allen Zones by 6-Month Period*

Tillman: The Tillman zones present a challenge because they significantly overlap due to two gangs operating in the same area, (see Figure 12). Therefore, discussing these two zones as one whole is misleading since offenses in the overlapping areas were double-counted (i.e., counted in the total for each zone, which inflates the total number and the number in each zone).

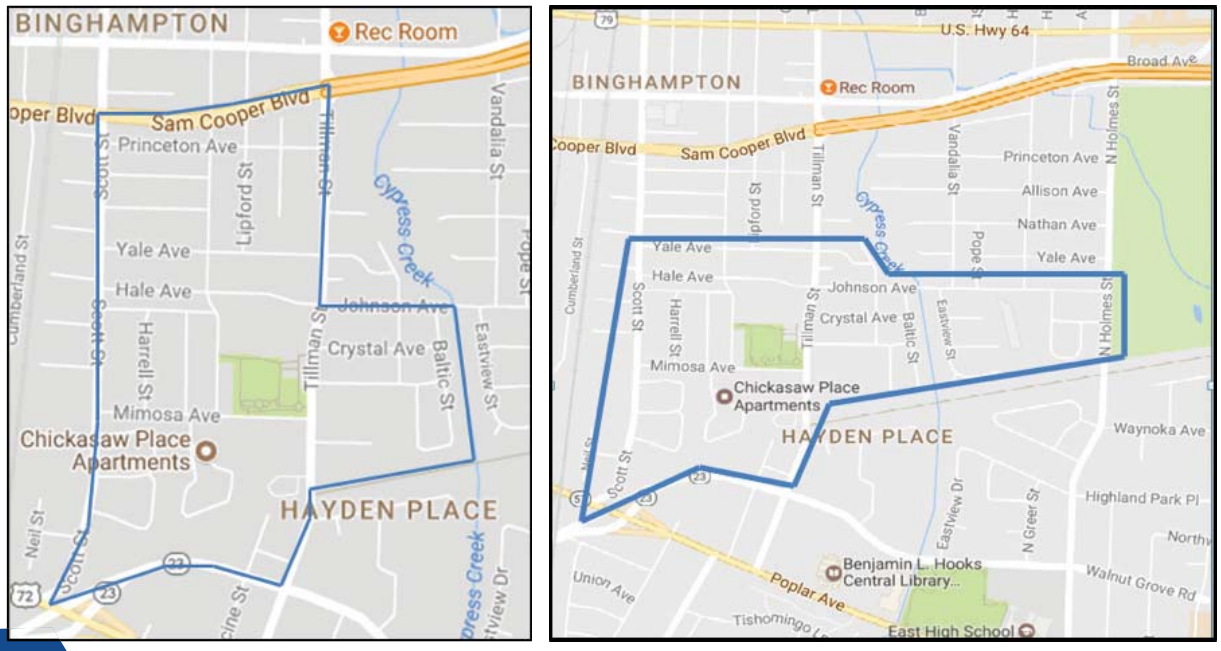

Figure 12: *Tillman Safety Zones: Grape Street Crips (left) and Vice Lords (right)*

Disregarding the overlap (which will be remedied in the full evaluation), the number of offenses in the Vice Lords zone decreased nearly 27 percent, while the number in the Grape Street Crips zone did not change, (see Figure 13). An increasing trend from the beginning of 2014 through the end of 2015 was seemingly stymied with the injunction in Jan. 2016 when violent offenses in the area dropped significantly. That decrease was short-lived, however, as numbers increased until they began declining again in July 2017.

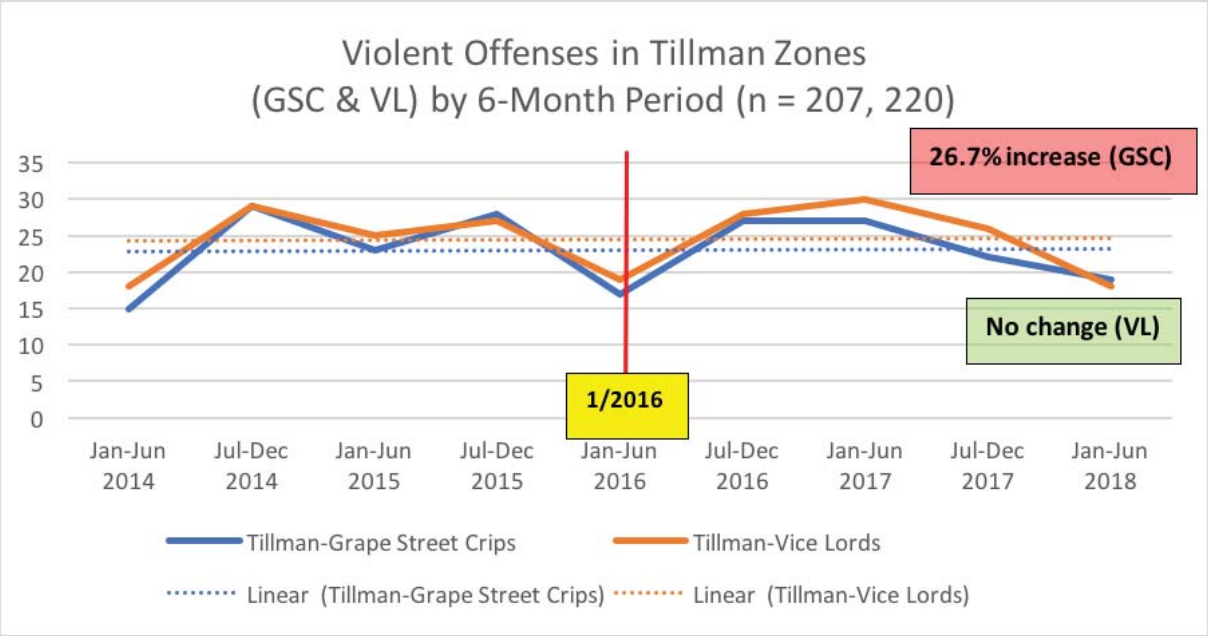

Figure 13: *Violent Offenses in Tillman Zones by 6-Month Period*

Arrests of Enjoined Individuals

According to the Shelby County District Attorney's Office, as of June 2, 2018, 67 actions were filed against 47 individuals for behaviors that violated the provisions of the gang injunctions. Of those 67 violations, 54 (80.6 percent) were dismissed or a *nolle prosequi* entered, five entered General Sessions Court guilty pleas, two were "held to state" (prepared for Criminal Court/Grand Jury indictment) and six had dispositions of "Null." The most common reason for disposition was "completed community service" (n=22), followed by time in jail (n=9) for between one and 44 days. Nine cases involved offenses that were disposed because of a more serious charge at the state or federal level.

For cases with dispositions, the average number of days between the individual involved receiving notice of the injunction and the date the court received the case was 493.64 days with a median of 449 days. This means that it took about 15–16 months for the average individual to be brought before the court for prohibited behavior. The average number of days between the date the court received the case and the disposition was 106.32 days with a median of 83 days. This means that the average case was disposed in around three months.

To determine the extent to which enjoined individuals have been committing violent offenses, MPD data on citywide arrests for violent offenses between Jan. 1, 2016 and Dec. 31, 2018 (three years) were examined and cross-referenced with enjoined individuals. During this period, 15 arrests of enjoined individuals for violent offenses were made (four in 2016, seven in 2017, four in 2018).

This same process was followed to determine the extent to which enjoined individuals had been committing violent gun offenses except the time period for examination was nine years, from Jan. 1, 2010 through Dec. 31, 2018. During this time, 35 enjoined individuals were arrested 37 times for violent gun offenses.

To examine any gun offense, including misdemeanor and weapons violations, the list of enjoined individuals was cross-referenced with an MPD list of citywide gun arrests from Jan. 1, 2014 through Dec. 31, 2018 (five years). During this time, 27 enjoined individuals had 33 arrests for any gun offense.

Finally, it is important to get a sense of the magnitude of criminal offending by all individuals identified as gang members. Data from MGU indicate that, during the eight months between April 1 and Nov. 31, 2018, 308 individuals identified by the MGU as gang members had 327 arrests for gun crimes. Nineteen individuals were arrested twice. This is an average of more than 40 per month. This includes seven arrests of six enjoined individuals, although these arrests could have occurred anywhere in the city and were not necessarily connected to their status as subject to injunction.

Officer Awareness

Officers both in injunction precincts (n=4) and in non-injunction precincts (n=5) were asked about their awareness and understanding of the injunction zones. Officers in the injunction precincts should have indicated awareness of the safety zones and of the behaviors prohibited by the gang injunctions. Blue bars in the graphs below indicate correct responses whereas red bars indicate incorrect responses. Charts illustrating responses for each precinct are shown below, beginning with the injunction precincts (Airways, Old Allen, North Main and Tillman).

Question 1 on the questionnaire filtered out respondents who were unaware of any safety zones in their precinct. If a respondent said "No" to Question 1, that respondent skipped all the other questions and only answered the last two questions ("time in service" and "rank").

Airways: A majority (65 percent) of Airways respondents indicated awareness of safety zones in the precinct. Of those who were aware (n=24), most did not know how many zones are in the precinct, and 92 percent did not know all 11 of the prohibited acts (see Figure 14). Most aware respondents correctly indicated that gang members cannot associate with each other in the zones, but fewer (54 percent) knew that gang members must be served notice of being subject to the injunction before they can be arrested for violations, and that they must stay away from alcohol in public in the zone (42 percent). Coming within 1,000 feet of a school in the safety zone is not a prohibited behavior, but this question was included as a distractor. Only three respondents (12.5 percent) correctly answered that question. Finally, just over half of respondents (54 percent) did not know that they should arrest a gang member they witness violating any of the 11 prohibitions.

The only gang covered by the Airways safety zone is Rollin' 90s, which was erroneously omitted from the first iteration of the questionnaire. However, six respondents knew enough to write-in "Rollin' 90s." Airways respondents who circled any other gang name were "incorrect," (see Figure 15).

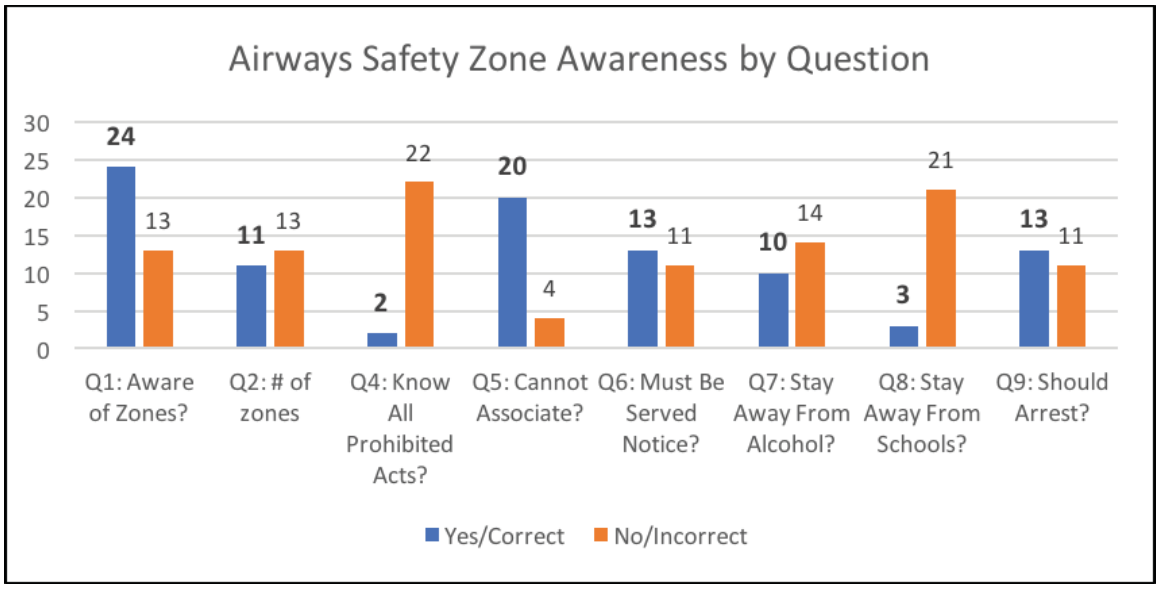

Figure 14: *Airways Safety Zone Awareness by Question*

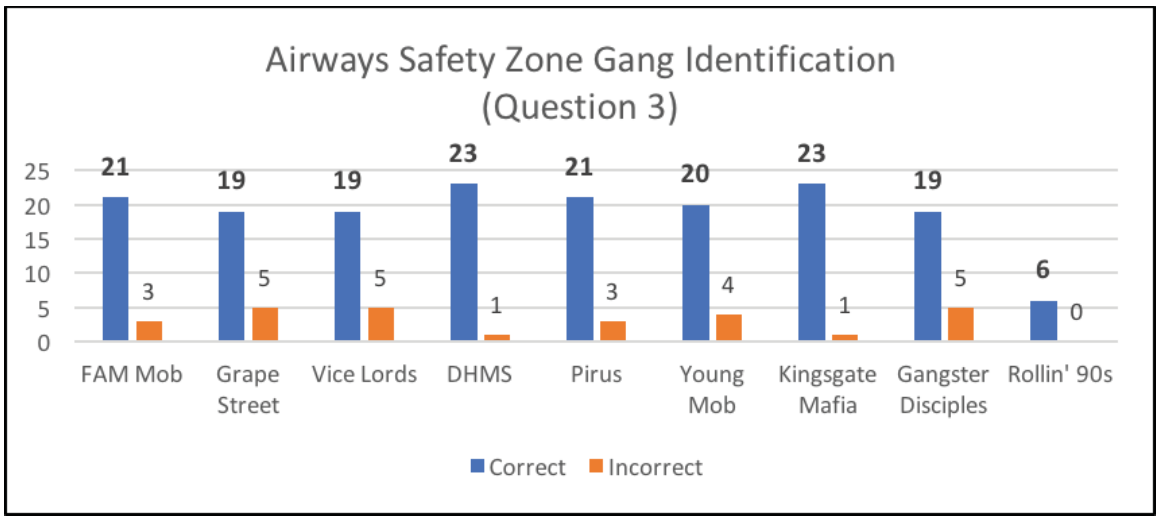

Figure 15: *Airways Safety Zone by Gang Identification*

Old Allen: A majority (65 percent) of Old Allen respondents indicated awareness of safety zones in the precinct (see Figure 16). However, most (54 percent) who indicated awareness did not know how many zones are in the precinct, and 85 percent did not know all 11 of the prohibited acts. Nearly all aware respondents correctly indicated that gang members cannot associate with each other in the zones (92 percent), fewer (65 percent) knew that gang members must be served notice of being subject to the injunction before they can be arrested for violations, and only half knew that gang members must avoid alcohol in public. Coming within 1,000 feet of a school in the safety zone is not a prohibited behavior, but this question was included as a distractor. Only four respondents (15 percent) correctly answered that question. Finally, most respondents (65 percent) knew they should arrest a gang member for violating any of the 11 prohibitions.

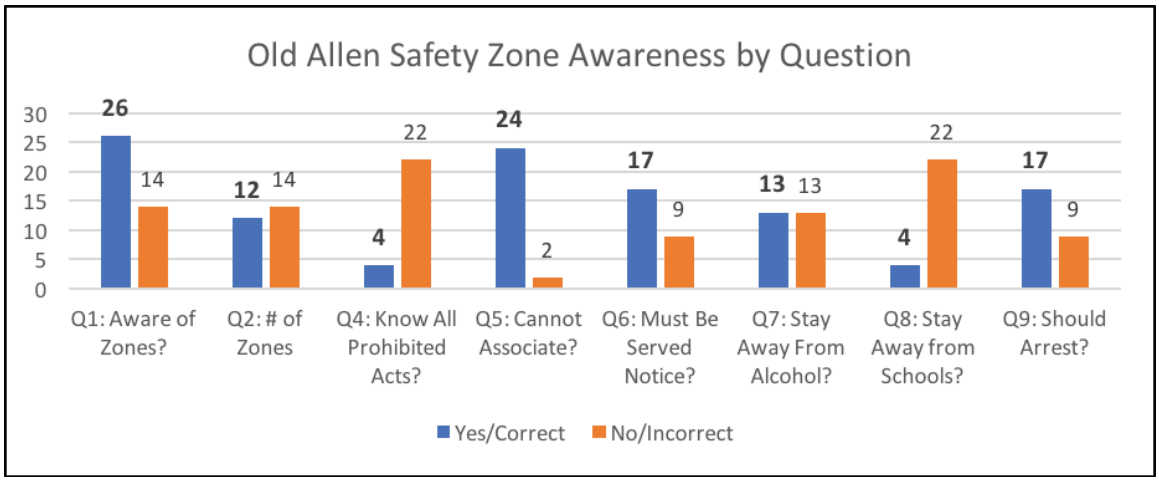

Figure 16: *Old Allen Safety Zone Awareness by Question*

Respondents who indicated awareness (n=26) were asked to identify all the gangs affected by Old Allen safety zones (see Figure 17). The only gang covered by the two Old Allen safety zones is FAM Mob. If a respondent indicated any other gang, they were "incorrect." If a respondent did not indicate any other gang, they were "correct." All respondents correctly identified FAM Mob and correctly did not identify DHMG and Kingsgate Mafia. Most (88 percent) knew that the Pirus were not covered, as well. However, more than one in three respondents (34.6 percent) incorrectly identified Vice Lords, Young Mob and Gangster Disciples as being covered in the OAS safety zones. An even greater percentage of respondents (42.3 percent) believed that the Grape Street Crips are covered in the Old Allen zones.

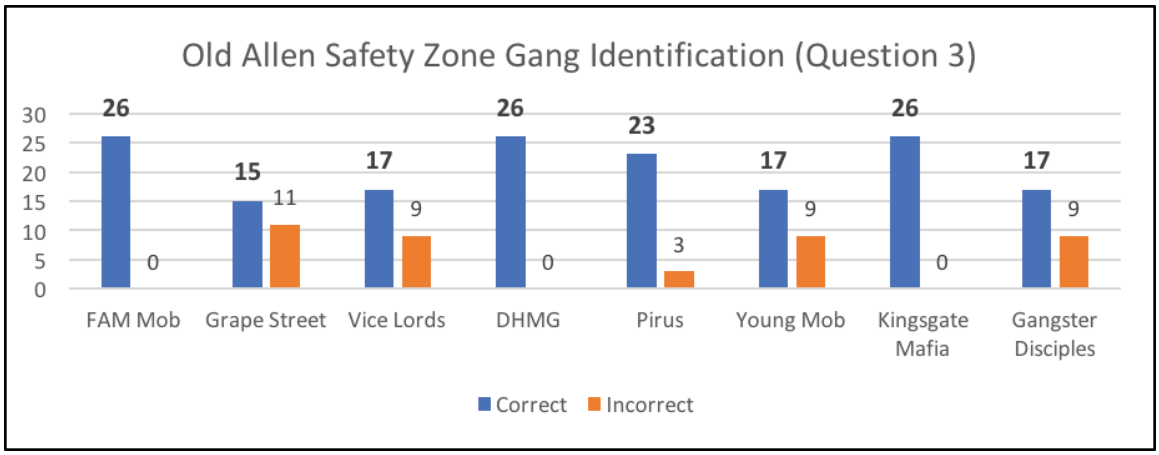

Figure 17: *Old Allen Safety Zone Gang Identification*

North Main: A majority (76.5 percent) of North Main respondents did not indicate awareness of safety zones in the precinct (see Figure 18). Of those who were aware (n=8), half did not know how many zones are in the precinct, and 87.5 percent did not know all 11 of the prohibited acts. Nearly all aware respondents correctly indicated that gang members cannot associate with each other in the zones and must avoid alcohol in public in the zones (87.5 percent), but fewer (75 percent) knew that gang members must be served notice of the injunction before they can be arrested for violations. Coming within 1,000 feet of a school in the safety zone is not a prohibited behavior, but this question was included as a distractor. Only one respondent correctly answered that question. Finally, most respondents (75 percent) did not know that they should arrest a gang member for violating any of the 11 prohibitions.

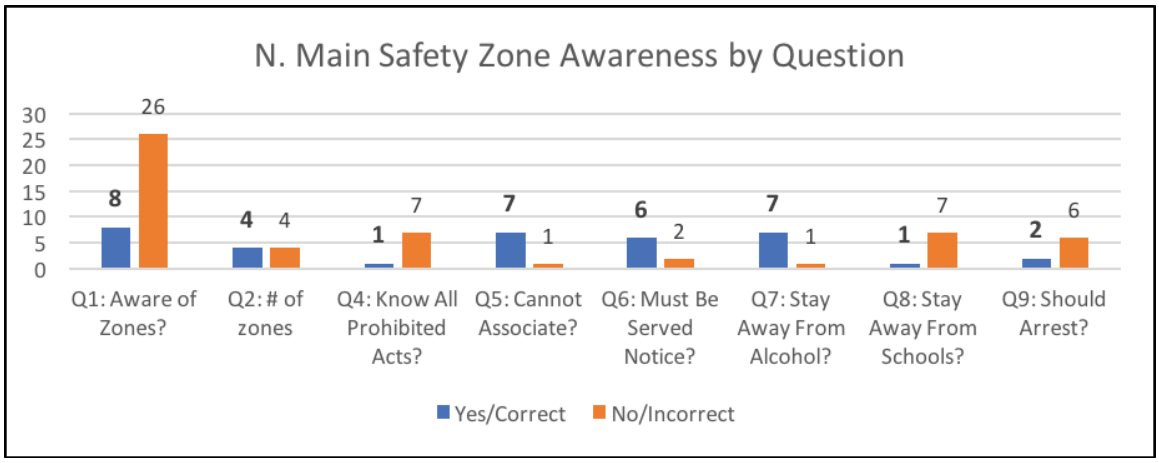

Figure 18: *N. Main Safety Zone Awareness by Question*

Respondents who indicated awareness (n=8) were asked to identify all the gangs affected by North Main safety zones (see Figure 19). The only gang listed in the options covered by the N. Main safety zone is Dixie Homes Murda Squad (DHMS). If a respondent indicated any other gang, they were "incorrect." If a respondent did not indicate any other gang, they were "correct." Most respondents correctly identified DHMS and correctly did not identify Pirus and Kingsgate Mafia. Most (62.5 percent) also knew that FAM Mob, Vice Lords, Young Mob and Gangster Disciples were not covered. However, three-fourths of respondents incorrectly identified Grape Street Crips as being covered in the North Main safety zones.

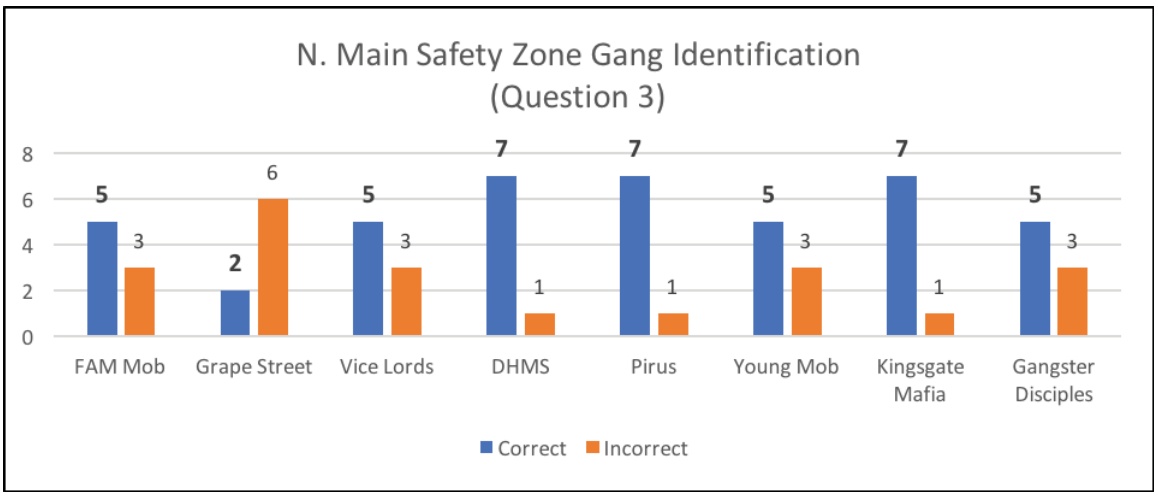

Figure 19: *N. Main Safety Zone Identification*

Tillman | Although Tillman has two safety zones, valid data from this precinct was not obtained. As a result, officer awareness in Tillman is not reported at this time. Tillman had 98 respondents, including three sergeants, six lieutenants and one major. The largest proportion of respondents (42 percent) had served more than 10 years.

Precincts Without Safety Zones | The Raines, Mt. Moriah, Crump, Appling Farms and Ridgeway precincts have no safety zones. Therefore, officers in the precincts should have said “no” to Question 1 and skipped to the last two questions.

Raines | Raines had 125 respondents, including 101 patrol officers, six sergeants, and nine lieutenants. The largest proportion of respondents (36 percent) had been with the MPD for more than 10 years, followed by those with six to 10 years (29 percent). Valid data from Raines was not obtained with respect to Question 1. As a result, officer awareness in Raines cannot be reported at this time.

Mt. Moriah | Mt. Moriah had 78 respondents, with 94 percent not aware of any safety zones. All respondents who indicated rank were patrol officers. The largest proportion of respondents (44 percent) had been with the MPD for one to five years, followed by those with six to 10 years of service (29.5 percent).

Crump | Of 81 respondents, 75 (93 percent) correctly indicated that they were not aware of any safety zones in their precinct. The largest proportion of respondents (38 percent) had been with the MPD for more than 10 years, followed by those with six to 10 years (24 percent). Of respondents who indicated rank, 70 were patrol officers and seven were sergeants.

Appling Farms | All 63 respondents (100 percent) correctly indicated that they were not aware of any safety zones in their precinct. The largest proportion of respondents (33 percent) had been with the MPD for less than a year followed by equal proportions at six to 10 years and more than 10 years (17 percent each). Nearly all respondents (94 percent) were patrol officers.

Ridgeway | Of 60 respondents, 57 (95 percent) correctly indicated that they were not aware of any safety zones in the precinct. The largest proportion of respondents (45 percent) had been with the MPD for more than 10 years followed by 23 percent having served between six to 10 years. Among the 50 respondents who indicated their rank were six sergeants and four lieutenants.

CONCLUSIONS

A full evaluation of the impact of gang injunctions will be conducted at the end of the five-year OSC-3 plan implementation period. This interim report, however, provides some interesting insight into the effectiveness of gang injunctions.

Three research questions guided the inquiry:

1) Do injunctions reduce the number of violent offenses in injunction areas? (Is there a general deterrent effect?)

2) Do gang injunctions reduce arrests of individuals subject to injunctions? (Is there a specific deterrent effect?)

3) Do officers working in precincts that have safety zones know about the injunctions and the prohibited behaviors?

Do injunctions reduce the number of violent offenses in injunction areas? (Is there a general deterrent effect?)

With the caveat that this analysis only considers post-injunction data and no control variables (i.e., trends from other parts of the city), it appears that gang injunctions and the establishment of six safety zones in four precincts has impacted the number of violent offenses within those zones.

From Jan. 1, 2014 until June 30, 2018, violent offenses in the zones dropped nearly 8 percent, and the average number of offenses dropped from .90 per week per zone to .83. The number of violent offenses decreased in four of the six zones. These decreases ranged from about 13 percent in North Main to more than 34 percent in Airways. The number of violent offenses in two zones (Old Allen-Greenbriar and Tillman-Grape Street Crips) did not change. Although a decrease is preferable, no change is still a positive result (i.e., violent offending did not increase).

Do gang injunctions reduce arrests of individuals subject to injunctions? (Is there a specific deterrent effect?)

Injunction violations. Since the first injunction in Sept. 2013, 47 enjoined individuals had been arrested for 67 injunction violations. More than 80 percent of those violations were dismissed or a *nolle prosequi* entered (most often occurring after completion of community service or some time in jail). Figure 20 below illustrates the number of violations brought before the court by month. It is not surprising to see peaks after injunctions, but violations should taper off over time if they have a specific deterrent effect. The full evaluation will be more instructive on whether violations decrease over time.

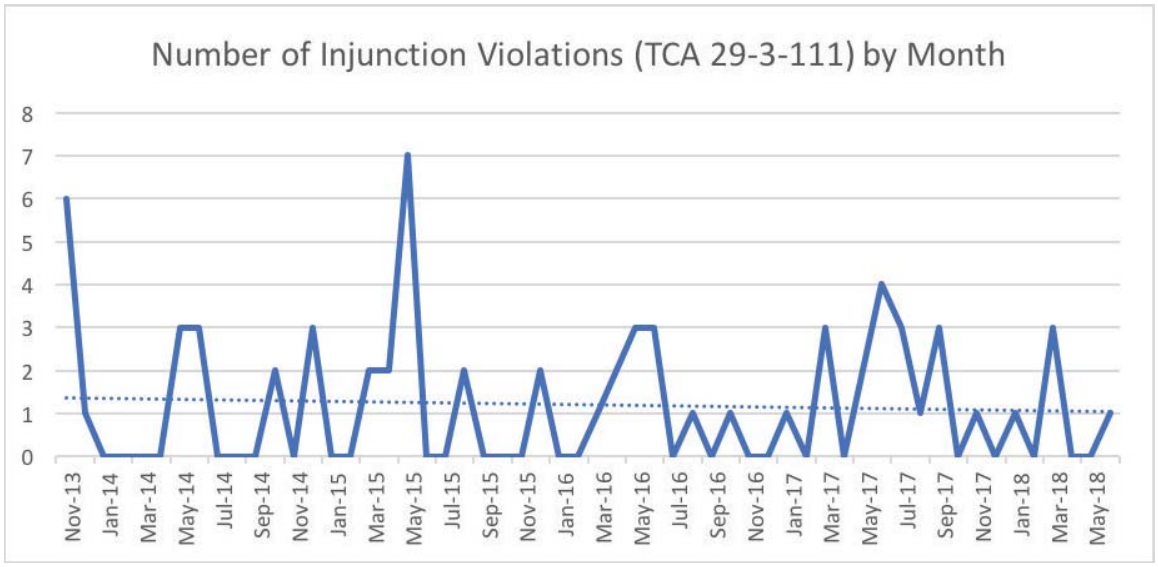

Figure 20: *Injunction Violations by Month (source: DA's Office)*

Arrests of enjoined individuals for violent, violent gun and any gun offense. Enjoined individuals were getting arrested for each type of offense: 15 were arrested for violent offenses during a three-year period (average of five per year); 35 were arrested for violent gun offenses during a nine-year period (average of 3.9 per year) and 27 were arrested for any gun crime during a five-year period (average of 5.4 per year). MGU data also indicate, that six enjoined individuals were arrested for gun crime in only eight months.

A post-injunction only investigation cannot determine whether injunctions have reduced arrests. It can only examine whether enjoined individuals have been arrested during the specified period and whether they were arrested in the safety zones. The full evaluation will more thoroughly address this research question by conducting, for each enjoined individual, a pre-injunction/post-injunction analysis of arrests going back as far as 2010 and tracked through 2021. Additionally, the full evaluation will map the locations of these arrests over time to determine if the injunctions reduced criminal offending or simply displaced it.

Do officers working in precincts that have safety zones know about the injunctions and the prohibited behaviors?

The preliminary answer to this question is no. While most officers in precincts without safety zones knew their precincts did not have safety zones, a significant proportion of officers in safety zone precincts were unaware of the zone(s). Among the four safety zone precincts, awareness among officers ranged from 24 percent to 65 percent. This means that between 35 percent and 76 percent were unaware. Moreover, if officers were aware of the zone(s), fewer were aware of the conditions of the injunctions or even the gang(s) covered under the injunction(s). If officers in a safety-zone precinct do not know about the safety zone(s), they will not be arresting individuals for injunction violations. Moreover, officers who do not know all the prohibited behaviors will underenforce injunctions, and officers who believe something is prohibited when it is not may attempt to enforce something that is not prohibited. The former has potential implications for public safety, and the latter has potential implications for community relations.

Nearly one-third of sworn MPD officers responded to the questionnaire, so it is a fair representation of the awareness of the department. However, it is not a perfect representation because respondents were not randomly selected. Some precincts were overrepresented and some precincts were underrepresented. Additionally, validity concerns with responses from Tillman and Raines required their exclusion from most analyses.

Limitations

Most agency data suffers from mistakes that need to be addressed. For example, no standard convention guides how officers enter names and/or addresses (e.g., “Jr.” versus “Junior,” “St.” versus “Street”). Dates are incorrectly entered. Names are misspelled. One entry includes the person’s middle initial while another one does not. This makes it extremely challenging to try to cross-reference individuals with other individuals across various databases. Although data was meticulously cleaned for this effort (i.e., approximately 40 hours to manually review and clean multiple databases), errors still are likely.

Mapping offenses in Tillman was complicated by the fact that the two safety zones overlap. This resulted in offenses committed within the overlapping areas being double counted, once in the Grape Street Crips zone and once in the Vice Lords zone. This will be remedied in the full evaluation by determining to which gang those offenses in the overlap area should be attributed.

Data from the MGU related to gang members arrested for gun crime also have limitations. MGU personnel expressed concerns about their accuracy, specifically that all gun arrests are not being captured. One senior MGU official described several situations in which gun arrests in Shelby County may not be accurately captured. As this official noted, “Two examples are gun arrests in Bartlett and Germantown. Neither are using [our records management system] as their reporting system, so we only capture their gun arrests if there was a federal trigger.” Gang members arrested for gun crimes in Collierville and Millington also may not be captured. The official also explained that in situations such as aggravated assault with a gun where the arrest is made later and no gun is recovered, that arrest “would not be captured.” This means that gun crime committed by gang members likely is being underreported.

Another limitation was that the Rollin’ 90s gang was inadvertently omitted from the questionnaire. While this only directly impacted the Airways Precinct, it affected the validity of the results. This has been remedied and any subsequent surveys will include that gang as an option.

Finally, there were validity concerns with questionnaire responses from Tillman and Raines requiring them to be excluded from analyses. In the future, the PSI will implement proactive measures to reduce the likelihood of this happening again.

RECOMMENDATIONS

Although no recommendations can be developed yet with respect to violent offenses or arrests in the safety zones, at least one recommendation is apparent at this point. The Memphis Police Department should consider additional training on gang injunctions and safety zones, especially within the Airways, Old Allen, North Main and Tillman precincts. Awareness of zones was spotty at best and dismal at worst. Lack of awareness could impact public safety and community relations. Officers should be provided information about which gangs and gang members are subject to the injunction(s), as well as the prohibitions of the injunctions. Additional training would sensitize the officers and make arrests for violations more likely.

REFERENCES

Decker, S. H., Melde, C. & Pyrooz, D. C. (2013). "What We Know About Gangs and Gang Members And Where Do We Go From Here?" *Justice Quarterly, 30*(3), 369-402.

Maxson, C.L., Hennigan, K.M. & Sloane, D.C. (2005). "'It's Getting Crazy Out There': Can a Civil Gang Injunction Change a Community?" *Criminology & Public Policy, 4*(3), 577-605.

National Gang Center (2016). *Brief Review of Federal and State Definitions of The Terms "Gang," "Gang Crime," and "Gang Member"* [PDF file]. Retrieved from: nationalgangcenter.gov/Content/Documents/Definitions.pdf.

O'Deane, M. & Morreale, S. (2011). "Evaluation of The Effectiveness of Gang Injunctions in California." *The Journal of Criminal Justice Research, 2*(1), 1-32.

Ridgeway, G., Grogger, J., Moyer, R. & MacDonald, J. (2018). "Effect of Gang Injunctions on Crime: A Study of Los Angeles from 1988-2014." *University of Pennsylvania Department of Criminology, Working Paper No. 2018-3.0.*

Rosenfeld, R., Bray, T. M. & Egley, A. (1999). "Facilitating Violence: A Comparison Of Gang-Motivated, Gang-Affiliated, and Nongang Youth Homicides." *Journal of Quantitative Criminology, 15*(4), 495-516.

Simpson, D. M. (2013). "'Injunctions 101' in the Gang Capital of the United States." *Los Angeles Magazine* (June 17). Available: lamag.com/citythinkblog/injunctions-101-in-the-gang-capital-of-the-united-states/

Tita, G. & Papachristos, A. (2009). "The Evolution Of Gang Policy: Balancing Suppression and Intervention." In R. Chaskin (Ed.), *Youth gangs and community intervention: Research, practice, and evidence.* New York: Columbia University Press.

Winton, R. & Queally, J. (2018). "Does the LAPD Still Need Gang Injunctions to Fight Crime? The City is About to Find Out." *Los Angeles Times* (March 17).

APPENDIX

Gang Injunction and Safety Zone Questionnaire

Instructions: *Operation Safe Community-3*, a 5-year plan to reduce crime in Memphis & Shelby County, has an objective that relates to law enforcement awareness of "injunctions," legal actions taken against gangs in some Precincts. Injunctions create "safety zones" and identify gang members subject to arrest if they engage in certain behaviors while in those zones. We are asking sworn officers in your Precinct to participate in this survey because your Precinct may have a safety zone. Your responses are anonymous and none of your responses will be used to identify you. **If you do not know an answer, please circle "don't know" rather than guessing**. This will help MPD improve training related to this subject. Thank you, in advance, for your participation.

PLEASE CIRCLE YOUR RESPONSE:

1. Are you aware of any safety zones in your Precinct?	YES NO **(If NO, skip to #10)**
2. How many safety zones are in your Precinct?	1 2 3 4 or more Don't know
3. What gangs are affected by those safety zones? **(You may circle more than one)**	FAM Mob Don't know Grape Street Crips Vice Lords Dixie Homes Murda Squad/47NHC Pirus Young Mob Kingsgate Mafia Gangster Disciples Rollin' 90's
4. Do you know ***all*** the 11 gang-member behaviors that are prohibited in the safety zones?	YES NO
5. Gang members subject to the safety zone prohibitions cannot associate with each other in public in the safety zone.	TRUE FALSE Don't know
6. A gang member must have been served notice before he/she can be arrested for violating the injunction.	TRUE FALSE Don't know
7. Gang members subject to the safety zone prohibitions must stay away from alcohol in public in the safety zone.	TRUE FALSE Don't know
8. Gang members subject to the safety zone prohibitions must not come within 1000 feet of a school in the safety zone.	TRUE FALSE Don't know
9. If you witness a gang member subject to the safety zone prohibitions violating one of the 11 prohibitions, what should you do? **(Circle ONLY one)**	Issue a citation Don't know Arrest them Call the MGU Call the District Attorney's Office Nothing. A citizen must report them.
10. What is your time in service with MPD?	Less than 1 year 1-5 years 6-10 years More than 10 years
11. What is your rank **(write in)**?	

memphis.edu/psi