BUTLER | SNOW

November 5, 2019

VIA ELECTRONIC MAIL

Honorable Jon P. McCalla
United States District Court Judge
Clifford Davis and Odell Horton Federal Building
167 North Main St.
Memphis, TN 38103

Re: *ACLU-TN v. City of Memphis,* Case No. 2:17-cv-02120-JPM-jay
Federal Agency Policies Regarding Use of Social Media for Investigative Purposes and Situational Awareness

Dear Judge McCalla:

Please accept this cover memorandum to the chart of **Federal Agency Policies Regarding Use of Social Media for Investigative Purposes and Situational Awareness,** submitted in connection with the Monitoring Team's Q3 Report. During the August 27, 2019, hearing before the Court, Your Honor requested information on the social-media monitoring policies of various federal agencies as a supplement to the survey of police department policies related to social media use across the country (*See* Ex. 6, Q2 Report, ECF No. 219-1, PageID No.7564.)

The Monitoring Team has researched the existence and nature of policies regarding the use of social media for investigative purposes and situational awareness for the following federal agencies:

- Bureau of Alcohol, Tobacco, Firearms & Explosives (ATF)
- Drug Enforcement Administration (DEA)
- Department of Homeland Security (DHS)
- Federal Bureau of Investigation (FBI)
- Federal Emergency Management Agency (FEMA)
- Internal Revenue Service Criminal Investigations (IRS)
- United States Marshals Service (Marshals Service)
- United States Postal Inspection Service (Postal Inspection Service)
- United States Secret Service (Secret Service)
- Social Security Administration (SSA)

For some of these agencies and departments, extensive information concerning their use of social media is available. In particular, for **DHS,** the Brennan Center for Justice at NYU School of Law earlier this year released a lengthy report concerning social media monitoring by Customs and Border Protection (CBP), Transportation Security Administration (TSA), Immigration 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

Customs Enforcement (ICE), and United States Citizenship and Immigration Services (USCIS). This report concluded that DHS "is rapidly expanding its collection of social media information and using it to evaluate the security risks posted by foreign and American travelers," and highlights methods of collection of social media information that include voluntary provision of social media identifiers, manual checks of accounts, and searches of border devices that may allow viewing of ordinarily-visible information or more detailed review or copying of the device's contents.

Additionally, for the **FBI**, several resources for its policies concerning online investigative practices are available on the internet, including the FBI's Domestic Investigations and Operations Guide (DIOG). The DIOG highlights the FBI's regulations regarding collection of information relating to the exercise of First Amendment rights, and details the online investigative methods FBI employees may use before and during various stages of investigations. FBI investigations range from assessments to preliminary investigations to full investigations, depending on the modicum of proof. In general, the FBI may use increasingly intrusive techniques as the level of investigation rises:

- Prior to opening an assessment, an FBI agent can search and review various forms of online information, including various government systems and paid-for-services databases, as well as information available to the public via the Internet. The use of fictitious information to register for access is prohibited, however. Information contained in a public chat room may fall within the category of "publicly available information." Also at this stage, an FBI employee may use his or her official email for the limited use of conducting a "clarifying interview" and must identify him- or herself as being affiliated with the FBI.

- In an assessment, an FBI agent may use all investigative methods authorized prior to the opening of an assessment, and may also use automated regular searches (e.g., Google alerts) to conduct regular searches of publicly available information. After an assessment is open, an FBI employee can also access private or restricted-access online forums if an exception to the search warrant requirement has been satisfied, such as through consent by a party with the authorization to access and control content on the site. This "consenting party" may be the account-holder for a social-networking site, a system administrator, or a company official with authority to direct others regarding site content. An FBI agent may also record or monitor online public, real-time communications, but not private, real-time communications, which are available only during predicated cases. In addition, an FBI agent should generally deal openly with the public during an assessment. That is, in general, an FBI agent cannot engage in undercover activity in an assessment because it is too invasive. He or she can, however, task sources to access a restricted website to gather information, if the source has authorized access (consent).

- In predicated investigations, which include preliminary investigations, full investigations, enterprise investigations, or positive foreign intelligence investigations, all online investigative methods authorized prior to the opening of an assessment or during an assessment are authorized, as well as additional online

methods such as (1) monitoring private, real-time online communications; (2) intercepting communications of a computer trespasser; and (3) undercover activity. The majority of the information concerning online investigative methods in undercover activity is redacted from the publicly available version of the DIOG.

The **IRS** also makes available online its Internal Revenue Manuals, which address the use of social networking sites for IRS employees engaged in both compliance work and criminal investigations. Although IRS employees engaged in compliance research may not register or use fictitious identities to access social networking websites, IRS employees engaged in criminal investigations may be permitted to assume a temporary pretext identity when accessing social networking websites for surveillance purposes. Any communication such as a "friend" request using a pretext identity requires an approved undercover operation.

Some information is available concerning **FEMA**. On March 10, 2016, FEMA produced a Privacy Impact Assessment for its Operational Use of Publicly Available Social Media for Situational Awareness. The Privacy Impact Assessment states that FEMA has an initiative using publicly available social media for situational awareness purposes. FEMA's Watch Centers collect information from publicly available media including social media websites and blogs and, although the initiative is not designed to actively collect personally identifiable information, FEMA's Watch Centers may collect, maintain, and disseminate limited amounts of personally identifiable information *in extremis* situations to prevent the loss of life or serious bodily harm.

We have thus far not been able to discover social media surveillance and use policies for the following agencies: **Secret Service**, **Marshals Service**, **ATF**, and **DEA**. Freedom of Information Act requests to discover their policies or relevant documents concerning social media use for investigations by various groups such as MuckRock.com, the Electronic Frontier Foundation, and the Electronic Privacy Information Center have been met with varying degrees of success. The enclosed chart explains and contains links to the documents that these groups were able to obtain via FOIA requests.

We also have thus far not able to discover any policies or FOIA requests for the **Postal Inspection Service** and **SSA**. Some reporting within the last year suggests that the SSA engages in social-media monitoring and is attempting to expand its ability to do so, but we have not found similar reporting with respect to the Postal Inspection Service.

Please advise if there is any additional information on these or other agencies that the Court would like.

Sincerely,

BUTLER SNOW LLP

Edward L. Stanton III