BRENNAN CENTER FOR JUSTICE

January 30, 2020

Re: Freedom of Information Law Request

Dear Sir or Madam:

This is a request under the California Public Records Act ("CPRA"), Cal. Gov't Code §§ 6250-6270, on behalf of the Brennan Center for Justice at NYU School of Law ("Brennan Center").

The Brennan Center seeks information relating to the Los Angeles Police Department's use of social media to collect information about individuals, groups, and activities, described below as "social media monitoring."

Background

In general, "social media monitoring" is a term describing the use of social media platforms like Facebook, Twitter, and Instagram to gather information for purposes including, but not limited to, identifying potential threats, reviewing breaking news, collecting individuals' information, conducting criminal investigations and intelligence, and gauging public sentiment.

Social media monitoring can be conducted through individual, direct use of social media platforms and their search functions (including via the use of a social media account, either public or undercover), or through third-party monitoring tools that use keywords, geographic locations, and data mining to identify trends and networks of association, such as Geofeedia or Dunami.

The Los Angeles Police Department ("LAPD") has engaged in social media monitoring since at least December 2014, at which time it employed "around 40 people to monitor social media manually."[1] This included "routinely crawl[ing] through social media" to monitor the profiles of persons of interest, including suspected gang members.[2] During that

[1] Edwin Chan & Alex Doibuzinskis, *U.S. Police Struggle to Uncover Threats on Social Media*, REUTERS (Dec. 26, 2014), https://www.reuters.com/article/us-usa-police-socialmedia/u-s-police-struggle-to-uncover-threats-on-social-media-idUSKBN0K40MD20141226.

[2] *Id.*

period, LAPD officers also wrote a grant application for the software Geofeedia,[3] a third-party social media monitoring platform that has been criticized for violating Facebook, Instagram, and Twitter's terms of service and facilitating the targeting of black rights protestors and Muslims.[4] It is unclear whether the LAPD ever used Geofeedia or similar tools.

Social media monitoring efforts are deeply susceptible to inherent bias and are often implemented in ways that have a disparate impact on marginalized communities and activists. For example, in 2016, Jasmyne Cannick—a well-known critic of the LAPD—discovered that officers had been monitoring her Twitter profile and the number of likes and retweets on one of her posts discussing a possible police involved shooting of a college student.[5] Such surveillance has a chilling effect on political speech, and potentially impinges upon First Amendment rights. In another example, LAPD officers have reported using social media to track teenagers' parties.[6] Given the troubling statistics on racial disparities in other police departments' surveillance of teenagers, particularly through the use of gang databases, the trend of using online platforms to track social gatherings merits further scrutiny.[7]

Despite widespread public interest in social media monitoring by law enforcement officers,[8] the public lacks information about the capabilities and limitations of the LAPD's social media monitoring operations. For this reason, we seek information about the

[3] Ally Marotti & Tribune News Services, *Twitter Cuts Off Chicago Startup Geofeedia After ACLU Reports Police Surveillance*, CHI. TRIBUNE (Oct. 11, 2016), https://www.chicagotribune.com/business/blue-sky/ct-twitter-suspends-geofeedia-access-bsi-20161011-story.html.

[4] *See, e.g.*, Alanna Durkin Richer, *Boston Police's Social Media Surveillance Unfairly Targeted Muslims, ACLU Says,* BOS. GLOBE (Feb. 7, 2018), https://www.bostonglobe.com/metro/2018/02/07/boston-police-social-media-surveillance-unfairly-targeted-muslims-aclu-says/9JUpzPmy8Tsr5RLxvCm61M/story.html; *Geofeedia Alerts*, PRIVACY SOS (Apr. 27, 2017), http://privacysos.org/wp-content/uploads/2018/02/Geofeedia-Alerts.pdf..

[5] Aaron Miguel Cantú, *Thin Blue Spin: How U.S. Cops Have Raided Social Media*, 32 BAFFLER 26, 34 (2016), https://www.jstor.org/stable/43959273.

[6] George Joseph, *How Police Are Watching You on Social Media*, CITYLAB (Dec. 14, 2016), https://www.citylab.com/equity/2016/12/how-police-are-watching-on-social-media/508991/.

[7] Emily Galvin-Almanza, *California Gang Laws are Normalized Racism*, APPEAL (Oct. 4, 2019), https://theappeal.org/drakeo-california-gang-laws-racism/; Becky Clarke, *Ban Police Gang Lists – They Are Racist and Unjust*, GUARDIAN (May 9, 2018), https://www.theguardian.com/commentisfree/2018/may/09/police-gang-lists-racist-black-matrix.

[8] *See, e.g.*, Ali Winston, *Did the Police Spy on Black Lives Matter Protesters? The Answer May Soon Come Out*, N.Y. TIMES (Jan. 14, 2019), https://www.nytimes.com/2019/01/14/nyregion/nypd-black-lives-matter-surveillance.html; Meredith Broussard, *When Cops Check Facebook*, ATLANTIC (Apr. 19, 2015), https://www.theatlantic.com/politics/archive/2015/04/when-cops-check-facebook/390882/; *Police: Social Media Surveillance*, BRENNAN CTR. FOR JUSTICE, https://www.brennancenter.org/issues/protect-liberty-security/social-media/police-social-media-surveillance (last visited Oct. 29, 2019).

Department's use of social media to collect information about individuals, groups, and activities. We therefore request the documents described below.

Request

The Brennan Center specifically requests records under the CPRA that were in the LAPD's possession or control from January 1, 2011 through the date of this request, in the following categories:

1. **Policies Governing Use**: Any and all policies, procedures, regulations, protocols, manuals, or guidelines related to the use of social media monitoring by police department employees for purposes other than conducting a background check for police department employment, including but not limited to conducting a criminal investigation, undertaking situational awareness activities, monitoring current or anticipated gatherings, or otherwise viewing or gathering information about individuals. This includes but is not limited to policies, procedures, manuals, or guidelines regarding the authorization, creation, use, and maintenance of fictitious or undercover online personas.

2. **Policies Governing Location Data Collection**: Any and all records, policies, procedures, regulations, protocols, manuals, or guidelines governing the collection and maintenance of location data from social media platforms and/or applications.

3. **Policies Governing Data Retention, Analysis, and Sharing**: Any and all records, policies, procedures, regulations, protocols, manuals, or guidelines relating to the retention, analysis, or sharing of data collected via social media.

4. **Recordkeeping**: Any and all recordkeeping, logs, or digests reflecting the use of social media monitoring or searches of social media for purposes including criminal investigations, situational awareness, event planning, or public safety.

5. **Third-Party Applications**: Any and all records reflecting a contract or agreement to purchase, acquire, use, test, license, or evaluate any product or service developed by any company providing third-party social media monitoring or analysis services, including but not limited to Geofeedia, Snaptrends, Firestorm, Media Sonar, Social Sentinel, or Dunami.

6. **Collection of Social Media Account Information**: Any and all records reflecting interactions with civilians in which police department employees requested information about the civilian's social media account information, including but not limited to a username, identifier, handle, linked email, or password.

7. **Civilian Communications**: Any and all records reflecting any communications conducted on social media platforms between uniformed or undercover police department employees and civilians, including but not limited to direct messages, group messages, chat histories, comments, or "likes," but excluding communications conducted as part of ongoing investigations and communications appearing on a page or account operated by the BPD and bearing the BPD's name, insignia, or other indicia of ownership or control.

8. **Use for Criminal Investigations**: Any and all records reflecting the number of criminal investigations in which social media research has been used, the number of criminal investigations in which fictitious/undercover online personas have been used, the nature of the offense(s) charged in each investigation, and the number of those investigations that resulted in arrests and/or prosecutions.

9. **Use for Purposes Other Than Criminal Investigations:** Any and all records reflecting the number of matters in which social media was used to collect information about individuals for purposes other than criminal investigations or background checks for police department employment, the nature of each such matter, the number of such matters in which an individual or group was charged with a crime, and the nature of each such matter.

10. **Audits**: Any and all records of, or communications regarding, audits or internal reviews of the Department's use of social media monitoring for the purpose of investigations, situational awareness, event planning, intelligence, or public safety, including but not limited to records reflecting any disciplinary actions, warnings, or proceedings in response to an employee's use of social media.

11. **Training Materials**: Any and all training documents (including draft documents) discussing social media monitoring, including but not limited to PowerPoint presentations, handouts, manuals, or lectures.

12. **Legal Justifications**: Any and all records reflecting the legal justification(s) for social media monitoring, including but not limited to memos, emails, and policies and procedures.

13. **Formal Complaints, Freedom of Information Requests, and Legal Challenges**: Any and all records reflecting formal complaints, Public Record requests, or legal challenges regarding the Department's use of social media monitoring, including, but not limited to, those complaints or legal challenges made by civilians, non-profit groups, companies, or the Community Ombudsman Oversight Panel.

14. **Federal Communications**: Any and all records reflecting any communications, contracts, licenses, waivers, grants, or agreements with any federal agency concerning the use, testing, information sharing, or evaluation of social media monitoring products or services.

15. **Nondisclosure Agreements**: Any and all records regarding the BPD's nondisclosure or confidentiality obligations in relation to contracts with third-party vendors of social media monitoring products or services.

16. **Vendor Communication:** Any and all records reflecting interactions with any third-party vendors concerning social media monitoring products or services, including, but not limited to, sales materials, communications, memorandums, and emails relating to those products.

17. **Metrics Measuring Effectiveness of Program:** Any and all reports, communications, metrics, or graphics representing the effectiveness of the Department's social media monitoring program, including but not limited to the degree to which use of social media monitoring led to the discovery of threats to public safety.

Fee Waiver and Expedited Processing

The above requests are a matter of public interest. Accordingly, the Brennan Center for Justice requests a fee waiver and expedited processing. The disclosure of the information sought is not for commercial purposes; instead, it will contribute to the public's understanding of government operations.

The Brennan Center for Justice is a nonpartisan, non-profit law and policy institute dedicated to upholding the American ideals of democracy and equal justice for all. The Center has a long history of compiling information and disseminating analysis and reports to the public about government functions and activities, including policing. Accordingly, the primary purpose of the above requests is to obtain information to further the public's understanding of important policing policies and practices. Access to this information is crucial for the Center to evaluate such policies and their effects.

Should the LAPD choose to charge a fee, please inform the Brennan Center if the cost will exceed $50.00, in writing at levinsonr@brennan.law.nyu.edu or Attn: Rachel Levinson-Waldman, 1140 Connecticut Ave. NW, Suite 1150, Washington, DC 20036.

Response Required

The Brennan Center appreciates the LAPD's attention to this request and expects that the LAPD will send its legally mandated response within ten business days of receipt, or

provide the date on which the response will be provided, as prescribed by the statute.[9] Should the LAPD determine that some portion of the documents requested contain exempt material, we request that the LAPD release those portions of the records that are not exempt. In addition, please provide the applicable statutory exemption and explain why it applies. We also request that you provide us with the documents in electronic format where possible.

Should you have any questions concerning this request, please contact Rachel Levinson-Waldman by telephone at (202) 249-7193 or via e-mail at levinsonr@brennan.law.nyu.edu.

[9] *See* Cal. Gov't Code § 6253(c).