BRENNAN CENTER FOR JUSTICE

January 30, 2020

Re: Freedom of Information Law Request

Dear Sir or Madam:

This is a request under the Maryland Public Information Act ("MPIA"), Md. Code, Gen. Prov. §§ 4-101 et seq., on behalf of the Brennan Center for Justice at NYU School of Law ("Brennan Center").

The Brennan Center seeks information relating to the Baltimore 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.

In 2016, records obtained through a Maryland Public Information Act request by the Baltimore Sun revealed that the Baltimore Police Department ("BPD") had employed a social media surveillance program called Geofeedia to monitor protests and other First Amendment-protected activities.[1] Geofeedia has touted its services to other police departments by citing the tool's use by the Baltimore County Police Department to monitor the social media posts and locations of protestors in the wake of Freddie Gray's death in

[1] Alison Knezevich, *Police In Baltimore, Surrounding Communities Using Geofeedia To Monitor Social Media Posts*, BALTIMORE SUN (Sep. 5, 2016), https://www.baltimoresun.com/news/investigations/bs-md-geofeedia-police-20160902-story.html.

2015.[2] Citing Gray's death as an "opportunity," Geofeedia contacted the Baltimore County Police Department and offered to "draw perimeters around key locations, set up automated alerts, and forward real-time information directly" to officers responding to protests.[3] The program aggregated data from at least eight social media platforms—including Facebook, Twitter, Instagram, and YouTube.[4] Information gleaned through Geofeedia was then put through facial recognition technology, allowing police officers to pull activists with outstanding warrants from the crowds of protesters and arrest them.[5]

The BPD and Baltimore County have defended their use of Geofeedia and social media monitoring writ large by claiming the data being accessed is already part of the public domain and therefore is not subject to privacy protections. Former BPD spokesperson T.J. Smith stated in 2016 that "[t]he only people that have anything to fear about anything being monitored are those that are criminals and attempting to commit criminal acts,"[6] and that social media monitoring "is not prying open a door of privacy."[7] Then-Baltimore Mayor Stephanie Rawlings-Blake made similar comments, arguing that "[w]hen we stay in the public domain, there's no expectation of privacy."[8] Notably, Instagram, Twitter, and Facebook all cut off Geofeedia's access to their data after the program's use by police departments came to light.[9] However, it is not known whether BPD continues to engage in social media monitoring through another third-party tool or the efforts of its own officers and detectives.

Despite widespread public interest in social media monitoring by law enforcement officers,[10] the public lacks information about the capabilities and limitations of the BPD's

---

[2] *See* Stephen Babcock, *Report: Police Worked With Social Media Company To Track Protestors During Unrest*, TECHNICALLY MEDIA (Oct. 12, 2016), https://technical.ly/baltimore/2016/10/12/geofeedia-baltimore-county-police/; Matt Cagle, *Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color*, ACLU (Oct. 11, 2016), https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target.

[3] *Baltimore County Police Department and Geofeedia Partner to Protect the Public During Freddie Grey Riots*, GEOFEEDIA, https://www.aclunc.org/docs/20161011_geofeedia_baltimore_case_study.pdf

[4] *Id*.

[5] Benjamin Powers, *Eyes Over Baltimore: How Police Use Military Technology to Secretly Track You*, ROLLING STONE (Jan. 6, 2017), https://www.rollingstone.com/culture/culture-features/eyes-over-baltimore-how-police-use-military-technology-to-secretly-track-you-126885/.

[6] Knezevich, *supra* note 1.

[7] Kate Amara, *ACLU Report: Baltimore Police Used Social Media Aggregator During Unrest*, WBALTV (Oct. 13, 2016), https://www.wbaltv.com/article/aclu-report-baltimore-police-used-social-media-aggregator-during-unrest/7148628.

[8] *Id*.

[9] Cagle, *supra* note 2.

[10] *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-

social media monitoring operations. For this reason, we seek information about the Department's use of social media to collect information about individuals, groups, and activities. We therefore request the documents below.

Request

The Brennan Center specifically requests records under the Public Information Act that were in the BPD's possession or control from January 1, 2014 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.

---

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).

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, a non-profit organization, requests a fee waiver pursuant to Md. Code, Gen. Prov. § 4-206(e).

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.

The Brennan Center has a limited ability to pay for charges associated with MPIA requests.[11] If the request for a waiver of fee is denied, please advise us in writing of the reason(s) for the denial and of the cost, if any, for obtaining a copy of the requested documents 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 BPD's attention to this request and expects that it will be fulfilled within 30 days as required by Md. Code, Gen. Prov. § 4-203(a). Should the BPD anticipate it will take more than 10 days to produce the requested records, we expect BPD will send its legally mandated response, setting out the amount of time anticipated to respond to the request, the expected fees, and the reason for the delay, no later than ten business days after receipt.[12] Should the BPD determine that some portion of the documents requested contain exempt material, we request that the BPD release those portions of the records that are not exempt.[13] 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.

[11] *See generally* Office of the Attorney General, Md. Pub. Info. Act Manual, 7-3 - 7-4 (14th ed. 2015) (discussing criteria for waiver of fees under the MPIA).

[12] *See* Md. Code, Gen. Prov. § 4- 203(b)(2)

[13] *See* Md. Code, Gen. Prov. § 4- 203(c).