

January 30, 2020

Re: Freedom of Information Law Request

Dear Sir or Madam:

This is a request under the Massachusetts Public Records Law, Mass. Gen. Laws, Ch. 66, § 10, on behalf of the Brennan Center for Justice at NYU School of Law (“Brennan Center”).

The Brennan Center seeks information relating to the Boston 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 2017, records obtained through the Massachusetts Public Records Law revealed that the Boston Police Department (“BPD”) had employed a social media surveillance system called Geofeedia to monitor the social media posts of Bostonians from 2014 to 2016, without the knowledge of the Boston City Council.¹ During this time, Geofeedia alerted the BPD to thousands of posts across at least seven social media platforms—including Facebook, Twitter, Instagram, and YouTube.² There is no indication that this surveillance

¹ See Iqra Asghar, *Boston Police Used Social Media Surveillance for Years Without Informing City Council*, ACLU.ORG (Feb. 8, 2018), <https://www.aclu.org/blog/privacy-technology/internet-privacy/boston-police-used-social-media-surveillance-years-without>.

² *Id.*

was ever instrumental in preempting terrorism or other violence.³ For example, one of Geofeedia’s monitoring targets was Tito Jackson, a city councilmember who posted on Facebook about racial inequality in Boston.⁴

The BPD also used Geofeedia to target the Muslim community. As part of a search for what analysts deemed “Islamist extremist terminology,” the BPD tracked commonplace Arabic words such as “ummah,” which means community.⁵ The targeting of speech related to cultural and religious communities raises serious civil rights concerns.

Moreover, the BPD also used Geofeedia to monitor First Amendment-protected activities, including protests and rallies. Indeed, BPD ended up using Geofeedia to track instances of social media posts that included phrases like “black lives matter,” “ferguson,” and “protest.”⁶ The BPD also surveilled individuals who protested Boston public school budget cuts using Geofeedia in 2016.⁷

At the same time, far less is publicly known about BPD’s social media monitoring via its own officers, detectives, or other employees rather than through the use of third-party services such as Geofeedia.

Request

The Brennan Center specifically requests records under the Public Records Law 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

³ *The Geofeedia Files: Boston Police And Social Media Surveillance*, PRIVACY SOS (2018), <https://privacysos.org/social-media-monitoring-boston-free-speech-crosshairs/>.

⁴ *Id.*

⁵ See Alanna Durkin Richer, *Boston Police’s Social Media Surveillance Unfairly Targeted Muslims*, *ACLU Says*, ASSOCIATED PRESS (Feb. 7, 2018), <https://www.bostonglobe.com/metro/2018/02/07/boston-police-social-media-surveillance-unfairly-targeted-muslims-aclu-says/9JUzPmy8Tsr5RLxvCm61M/story.html>.

⁶ See *Geofeedia Alerts*, PRIVACY SOS (Apr. 27, 2017), <http://privacysos.org/wp-content/uploads/2018/02/Geofeedia-Alerts.pdf>.

⁷ See Asghar, *supra* note 1.

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, a non-profit organization, requests a fee waiver pursuant to 950 C.M.R. § 32.06.

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 BPD 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 BPD's attention to this request and expects that the BPD will send its legally mandated response no later than ten business days after receipt.⁸ 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. 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.

⁸ See G.L. c. 66, § 10 (a-b); 950 CM 32.06.