

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.wbal.tv.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, Snaprends, 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).



BALTIMORE POLICE DEPARTMENT



Bernard C "Jack" Young
Mayor

Michael S Harrison
Police Commissioner

October 20, 2020

Sahil Singhvi
Research & Program Associate, Liberty and
National Security Program Brennan Center for
Justice at NYU School of Law (DC office)
1140 Connecticut Ave. NW, Suite 1150
Washington, DC 20036
singhvis@brennan.law.nyu.edu

Re: MPIA Request 20-0187

Dear Mr. Singhvi,

You have made a request for public records pursuant to the Maryland Public Information Act (MPIA), which is the General Provisions Article, § 4-101, et seq., of the Annotated Code of Maryland. You requested the Baltimore Police Department's ("BPD") records related to social media monitoring operations in BPD's possession or control from January 1, 2014 through the date of this request, for the following categories below.

Please note, due to the complexity of your request BPD had to contact several different departments within the agency to attempt to find responsive records. Also, please note teleworking caused BPD to have a delay with its response due to COVID-19, the Governor's Executive Orders, national public health guidance, and social distancing.

In addition, portions of the request are vague and ambiguous and needs more clarification. Nonetheless, please find below BPD's best response to your request.

Request #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.

Response #1: BPD does not have general comprehensive policies, procedures, regulations, protocols, manuals, or guidelines governing the use of social media for conducting a criminal investigation, undertaking situational awareness activities, monitoring current or anticipated gatherings, or otherwise viewing or gathering information about individuals. However, BPD has a policy to guide all members of the Baltimore Police Department (BPD) in the professional use of social media, and personal use of social media, only to the extent that personal use of social media sites or platforms may bear on a member's official duties found under Policy 604 (see attached). BPD also, has a policy that states social media should be lawfully collected during an overdose case from cellphones to help investigators identify the possible source of CDS found under Policy 801 (see attached). Detectives/Officers conduct their own investigations using social media accounts. As for policies, procedures, manuals, or guidelines regarding the authorization, creation, use, and maintenance of fictitious or undercover online personas, this information would be considered classified and confidential because of its sensitive nature. Maryland Code, General Provisions, Section 4-352 authorizes denial of records related to emergency management, including "response procedures or plans prepared to prevent or respond to emergency situation, the disclosure of which would reveal vulnerability assessments, specific tactics, specific emergency procedures, or specific security procedures." Likewise, section 4-351 authorizes denial of records of security procedures by a police department where disclosure would "interfere with a valid and proper law enforcement proceeding" or "endanger the life or physical safety of an individual."

Request #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.

Response #2: BPD does not have policies, procedures, regulations, protocols, manuals, or guidelines governing the collection and maintenance of location data from social media platforms and/or applications.

Request #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.

Response #3: BPD does not have policies, procedures, regulations, protocols, manuals, or guidelines relating to the retention, analysis, or sharing of data collected via social media.

Request #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.

Response #4: BPD does not have 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 that would be kept in a central location. This would be kept on an individual bases. In addition, this portion of your request would be considered unreasonably and burdensome. BPD is only able to comply with requests that the Custodian of Records is able to identify and locate by a process that is not unreasonably burdensome or disruptive of BPD operations. Therefore, the BPD cannot conduct wide-ranging and unreasonably burdensome searches for records. Furthermore, BPD has the authority to deny this portion of your request as too burdensome. *See, Ruotolo v. Dep't of Justice, Tax Div.*, 53 F.3d 4, 9 (2d Cir. 1995). Likewise, the PIA does not impose an obligation on a custodian to create a document that is responsive to a request. *See* MPIA Manual 13th Ed., October 2014, 3 (citing *Yeager v. DEA*, 678 F.2d 315, 324 (D.C. Cir. 1982)) (“[City] has no obligation to *create* records to satisfy a[n] [M]PIA request.”); *see also MacPhail v. Comptroller of Maryland*, 178 Md. App. 115, 119 (2008) (explaining that pertinent Federal Freedom of Information Act (“FOIA”) cases are “persuasive” authority in Maryland because the MPIA and the FOIA share “virtually identical” purposes.”).

Request #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.

Response #5: The responsive records are maintained by the Watch Center under BPD. To this end, please find attached the Requisition Geofeedia Renewal, Baltimore Police Department Proposal, Geofeedia Order Form and Purchase Order.

Request #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.

Response #6: See response #4.

Request #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.

Response #7: See responses #1 and #4. In addition, communications between civilians and undercover members of BPD cannot not be disclosed because it would be considered classified and confidential information.

Request #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.

Response #8: See response #4.

Request #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.

Response #9: See response #4.

Request #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.

Response #10: BPD does not have any 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. As far as "disciplinary actions, warnings, or proceedings in response to an employee's use of social media" This portion of the records sought are protected personnel records under Maryland Law. See Md. Code Ann., General Provisions Art. ("GP"), § 4-101 *et seq.* Further, the Maryland Court of Appeals in *Montgomery County v. Shropshire* noted that the "personnel" exception to disclosure includes documents "relating to hiring, discipline, promotion, dismissal, or any other matter involving an employee's status." 420 Md. 362, 378 (2011). Inspection is permissible only by the person in interest or an elected or appointed official that supervises the individual's work. See GP, § 4-311(b)(1)(2) (2014).

Request #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.

Response #11: BPD does not have any training documents (including draft documents) discussing social media monitoring, including but not limited to PowerPoint presentations, handouts, manuals, or lectures.

Request #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.

Response #12: If any such documents existed, the documents would be considered privileged and confidential under the attorney-client and/or work-product privilege.

Request #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, nonprofit groups, companies, or the Community Ombudsman Oversight Panel.

Response #13: The responsive records are maintained by the Public Integrity Bureau ("PIB") and the Document Compliance Unit ("DCU") under BPD. To this end, please find attached two Maryland Public Information Act ("MPIA") requests regarding social media under our tracking numbers MPIA 18-1270 and 18-0807. BPD didn't have responsive records for MPIA 18-1270 and for MPIA 18-0807 BPD sent Policy 604. Also, please find attached, an excel spreadsheet titled, "Social Media PIA-For Release" in regards to the formal complaints. Furthermore, upon information and belief, BPD is not aware of any lawsuits filed against the Department regarding social media monitoring.

Request #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.

Response #14: BPD does not have any 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.

Request #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.

Response #15: BPD does not have any records regarding the BPD's nondisclosure or confidentiality obligations in relation to contracts with third-party vendors of social media monitoring products or services.

Request #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.

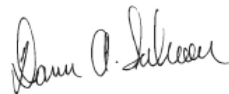
Response #16: See response # 5.

Request #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.

Response #17: See response #4.

The PIA, Annotated Code of Maryland, General Provisions Article, § 4-206 provides that the official custodian may charge "reasonable fees" for copies. However, the fees associated with your request have been waived. You have the right under PIA § 4-1B-04 to contact the Public Access Ombudsman to mediate any dispute(s) you may have with this response. You may also, contest this response by filing a complaint for Judicial Review in Circuit Court pursuant to PIA § 4-362. Please refer to MPIA tracking # **20-0187** in any subsequent correspondence pertaining to this matter.

Sincerely,

A handwritten signature in black ink, appearing to read 'Dana A. Saboor', is positioned above the printed name.

Dana Abdul Saboor
Paralegal
Baltimore Police Department
Document Compliance Unit



Baltimore Police Department | 9/10/2013

What is Geofeedia?

Geofeedia is a location-based social media monitoring, analysis and engagement platform.

Our solution enables Law Enforcement agencies to understand, in real-time, social media happening at locations important to them. Our patent-pending technologies allow you to search and monitor areas as large as a city or as small as a single building across multiple social media services.

We search by geo-location first rather than by specific keywords. We complement traditional social media keyword monitoring tools as our data set contains a significant amount of social content typically missed by keyword monitoring.

How Does It Work?

Through our simple point and click map drawing interface, you define specific locations to search and monitor. We deliver all geo-tagged social media from the locations you define to your desktop as real-time snapshots or perpetual monitoring streams. We provide analytics and sharing tools, and archive the content you capture in our secure data warehouse. You can retrieve historical content, or export data in a variety of formats.

What's the Benefit?

Many Law Enforcement agencies use us to improve:

- Targeted surveillance and monitoring
- Crisis response and management
- Resource Allocation
- Digital investigation
- Venue security operations
- Community engagement

This proposal (the "Proposal") will serve to confirm Customer's order for the services described above ("Services") for the prices listed herein. Customer's use of the Services is subject to the terms and conditions of Geofeedia's Online Terms of Use (www.geofeedia.com/termsfuse). Payment terms. On the effective date, Geofeedia will invoice Customer for all fees indicated above. The fees indicated above are effective for the Initial Term. Thereafter, Geofeedia may change any of the fees indicated above, with such changes being effective at the conclusion of the then-current term, by providing Customer with notice of such changes at least thirty (30) days prior to the end of the then-current term. The contract will automatically renew at the end of the term specified unless either party terminates in writing with 30 days notice prior to the end of the then-current term.

Baltimore Police Department | 9/10/2013

Base Application License

Included

Real Time Search

- ✓ Search social media sources by location and view results in our map or collage views
- ✓ Unlimited data from monitored Geofeeds per this proposal, otherwise limited to the last 24 hours

Analytics

- ✓ Filtering by keyword and user; trend views by volume, media, keyword and user; detailed view of feed items and associated metadata; curate items in collections

Archive and Export

- ✓ Share results via social media or email
- ✓ Unlimited monitored Geofeed and collection archival in secure data warehouse
- ✓ Export and access Geofeed results from monitored locations in ATOM/GeoRSS, JSON, or CSV format

Streaming

- ✓ View up to five concurrent live streams of social media per licensed user

Location Monitoring

Included

- ✓ Geofeedia will continuously monitor and record social media from user defined locations providing the ability to perform historical searches and analysis
- ✓ Ability to change monitored locations in real-time
- ✓ See below to determine number of monitored locations

User Licenses and Data Charges

Included

- ✓ See below to determine number of user licenses
- ✓ No data charges (thresholds apply at 10,000 feed items per month total monitored locations for Option A, 20,000 feed items per month for Option B, and 30,000 items for Option C. Additional data packs available at \$100 per thousand items).

Support and Training

Included

- ✓ Account set-up and initial location monitoring configuration
- ✓ One kick-off training session plus one user-training session per month when requested
- ✓ Priority customer support

Terms

- ✓ Initial Term: 12 months
- ✓ Full payment due upon signing
- ✓ 20% discount available on multi-year term

This proposal (the "Proposal") will serve to confirm Customer's order for the services described above ("Services") for the prices listed herein. Customer's use of the Services is subject to the terms and conditions of Geofeedia's Online Terms of Use (www.geofeedia.com/termsfuse). Payment terms. On the effective date, Geofeedia will invoice Customer for all fees indicated above. The fees indicated above are effective for the Initial Term. Thereafter, Geofeedia may change any of the fees indicated above, with such changes being effective at the conclusion of the then-current term, by providing Customer with notice of such changes at least thirty (30) days prior to the end of the then-current term. The contract will automatically renew at the end of the term specified unless either party terminates in writing with 30 days notice prior to the end of the then-current term.

Option A: 1 year term

1 user licenses (\$100/month)	\$1,200
3 monitored locations (\$100/location/month)	\$3,600
Setup	(Waived)
Total ANNUAL INVESTMENT	\$4,800

Option B: 1 year term

2 user licenses	\$2,400
5 monitored locations	\$6,000
Strategic Partner Discount – 10%	(\$840)
Setup	(Waived)
Total ANNUAL INVESTMENT	\$7,560

This proposal (the "Proposal") will serve to confirm Customer's order for the services described above ("Services") for the prices listed herein. Customer's use of the Services is subject to the terms and conditions of Geofeedia's Online Terms of Use (www.geofeedia.com/termsfuse). Payment terms. On the effective date, Geofeedia will invoice Customer for all fees indicated above. The fees indicated above are effective for the Initial Term. Thereafter, Geofeedia may change any of the fees indicated above, with such changes being effective at the conclusion of the then-current term, by providing Customer with notice of such changes at least thirty (30) days prior to the end of the then-current term. The contract will automatically renew at the end of the term specified unless either party terminates in writing with 30 days notice prior to the end of the then-current term.

Option C: 1 year term

2 user licenses	\$2,400
7 monitored locations	\$8,400
Strategic Partner Discount – 10%	(\$840)
Setup	(Waived)
Total ANNUAL INVESTMENT	\$9,960

Option D: 1 year term

2 user licenses	\$2,400
10 monitored locations	\$12,000
Strategic Partner Discount – 15%	(\$2,160)
Setup	(Waived)
Total ANNUAL INVESTMENT	\$12,240

Option Selected: _____

Signed: _____

Printed Name: _____

Title: _____

Date: _____

This proposal (the "Proposal") will serve to confirm Customer's order for the services described above ("Services") for the prices listed herein. Customer's use of the Services is subject to the terms and conditions of Geofeedia's Online Terms of Use (www.geofeedia.com/termsfuse). Payment terms. On the effective date, Geofeedia will invoice Customer for all fees indicated above. The fees indicated above are effective for the Initial Term. Thereafter, Geofeedia may change any of the fees indicated above, with such changes being effective at the conclusion of the then-current term, by providing Customer with notice of such changes at least thirty (30) days prior to the end of the then-current term. The contract will automatically renew at the end of the term specified unless either party terminates in writing with 30 days notice prior to the end of the then-current term.

This proposal (the "Proposal") will serve to confirm Customer's order for the services described above ("Services") for the prices listed herein. Customer's use of the Services is subject to the terms and conditions of Geofeedia's Online Terms of Use (www.geofeedia.com/termsfuse). Payment terms. On the effective date, Geofeedia will invoice Customer for all fees indicated above. The fees indicated above are effective for the Initial Term. Thereafter, Geofeedia may change any of the fees indicated above, with such changes being effective at the conclusion of the then-current term, by providing Customer with notice of such changes at least thirty (30) days prior to the end of the then-current term. The contract will automatically renew at the end of the term specified unless either party terminates in writing with 30 days notice prior to the end of the then-current term.

ORDER FORM

Order Information

Account Name: Baltimore Police Department
Prepared By: Trent McMahan

Contract Start Date: 11/1/2015
Contract End Date: 10/31/2016

Total Amount: [\$18,000.00]

Subscription Term, Billing & Payment Information

Company Name: Baltimore Police Department
Billing Name: Sgt. William MacDonald
Billing Email: William.macdonald@baltimorepolice.org
Billing Address: 242 W. 29th St.
Baltimore, MD 21211-2908

Billing Phone: (410) 396-2640

Billing Fax:

Payment Method: Invoice

PO Number: [IF APPLICABLE]

Billing Terms: Invoices sent *Annually*

Payment Terms: Due Upon Receipt. Interest accrues at the rate of 1.5% per month 60 days after the invoice date.
Invoices 30 days or more past due may result in suspension of Services.

This Order Form is subject to and governed by the terms and conditions of the Geofeedia Service Agreement posted online at <http://www.geofeedia.com/legal/service-agreement/> (unless there is already a Geofeedia Service Agreement in force and effect between you and Geofeedia, in which case the terms of such existing Geofeedia Service Agreement shall govern this Order Form). If for any reason you are unable to view the Geofeedia Service Agreement online at http://www.geofeedia.com/legal/master_agreement, please contact Geofeedia immediately.

Customer: _____

Geofeedia, Inc.

Signature: _____

Signature: _____

Printed: _____

Printed: _____

Title: _____

Title: _____

Date: _____

Date: _____

Application Services Subscription*

The Application Services include the following:

<u>Service Edition</u>	<u>Total Price</u>
------------------------	--------------------

Standard Service Package

Customer orders the following Standard Service Package:

Geofeedia Professional Edition

\$ 18,000.00

Total Permitted Users: Thirty (30)

Standard Applications

- Real-Time Search
- Up to five (5) Real-Time Streams
- Administrator functions

Premium Applications

- Geofeed Manager (Unlimited)
- Collections
- One-click Instagram Widget
- Alerts
- Influencers

Other Included Features

- Shape File Support
- Language Translations
- Data Export
- Analytics
- Networks currently Included: Instagram, Twitter, Flickr, Picasa, YouTube, Facebook, Sina Weibo, VK

Data Storage**

- Up to 250,000 post per month

Search Radius

- Maximum of 15 kilometers

Additional options

N/A

None

Training and Implementation

N/A

Total Annual Cost

\$ 18,000.00

Order Comments

* Assuming no Overage Fees.

** Data overage will be billed at a cost of \$50.00 per 1,000 posts in excess of per-month allowance.

Note: Any other services not included hereunder and must be identified in a separately executed Statement of Work.

For additional details regarding standard features and functionality of the Application Services, please visit:

<http://geofeedia.com/how-it-works>

From: 57679-26624274@requests.muckrock.com
Sent: Monday, July 09, 2018 10:59 AM
To: DCU
Subject: Maryland Public Information Act Request: Social Media Monitoring policies (Baltimore Police Department)

Follow Up Flag: Follow up
Flag Status: Flagged

Baltimore Police Department
PIA Office
room 100
100 Holliday Street
Baltimore, MD 21202

July 9, 2018

To Whom It May Concern:

Pursuant to the Maryland Public Information Act, I hereby request the following records:

Copies of your Agency's social media monitoring policies and guidelines, as well as any assessments of its privacy or legal implications.

I am a member of the news media and request classification as such. I have previously written about the government and its activities, with some reaching over 100,000 readers. As such, as I have a reasonable expectation of publication and my editorial and writing skills are well established. In addition, I discuss and comment on the files online and make them available through non-profits such as the Internet Archive and MuckRock, disseminating them to a large audience. While my research is not limited to this, a great deal of it, including this, focuses on the activities and attitudes of the government itself. As such, it is not necessary for me to demonstrate the relevance of this particular subject in advance.

As my primary purpose is to inform about government activities by reporting on it and making the raw data available, I request that fees be waived.

The requested documents will be made available to the general public, and this request is not being made for commercial purposes.

In the event that there are fees, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not.

Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 10 calendar days, as the statute requires.

Sincerely,

Emma Best

Filed via MuckRock.com

E-mail (Preferred): 57679-26624274@requests.muckrock.com

Upload documents directly: https://www.muckrock.com/accounts/agency_login/baltimore-police-department-646/social-media-monitoring-policies-baltimore-police-department-57679/?uuid-login=4ba2f81a-acbe-4166-8185-1a62d5156bb5&email=DCU%40baltimorepolice.org#agency-reply

Is this email coming to the wrong contact? Something else wrong? Use the above link to let us know.

For mailed responses, please address (see note):

MuckRock News

DEPT MR 57679

411A Highland Ave

Somerville, MA 02144-2516

PLEASE NOTE: This request is not filed by a MuckRock staff member, but is being sent through MuckRock by the above in order to better track, share, and manage public records requests. Also note that improperly addressed (i.e., with the requester's name rather than "MuckRock News" and the department number) requests might be returned as undeliverable.



Conner, David

From: DCU
Sent: Friday, October 19, 2018 6:33 AM
To: Conner, David
Subject: FW: follow up on FOIA request

Respectfully,

Officer Kenneth Hurst I411
Baltimore Police Department
Document Compliance Unit
Legal Affairs Division
242 W. 29th Street
Baltimore, MD 21211
DCU@baltimorepolice.org
MPIA request forms
<http://law.baltimorecity.gov/office-legal-affairs-baltimore-police-department>

CONFIDENTIALITY NOTICE: The information contained in or attached to this e-mail message may be a privileged and confidential attorney/client communication, or otherwise confidential, and is intended only for the use of the individual or entity to whom it is addressed. If you are not the intended recipient, or the employee or agent responsible for delivering the message to the intended recipient, you are notified that any distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify the Legal Affairs Division immediately by telephone at 410-396-2496 and DELETE the message from your system immediately.

The materials in this e-mail are private and may contain sensitive law enforcement information. Please note that e-mail is not necessarily confidential or secure. Use of e-mail constitutes your acknowledgment of these confidentiality and security limitations. If you are not the intended recipient, be advised that any unauthorized use, disclosure, copying, distribution, or the taking of any action in reliance on the contents of this information is strictly prohibited as covered by the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2521. If you have received this e-mail in error, please immediately notify the sender via telephone or return e-mail.

From: Anne Branigin [mailto:anne.branigin@theroot.com]
Sent: Thursday, October 18, 2018 4:39 PM
To: DCU; news@baltimorepolice.org
Cc: Kashmir Hill
Subject: follow up on FOIA request

Hello,

Kashmir Hill and I are reporters with Gizmodo Media Group. We submitted a freedom of information request to Baltimore PD on August 16th but have not yet received a response. I am getting in touch to ask whether the Baltimore Police Department uses undercover accounts on social media as an investigative technique and whether it has any type of

internal rules or department policy for covert operations on social media (i.e. the creation of fictitious accounts on social networks like Facebook, Instagram, or Twitter that are used to friend persons of interest to get access to their social postings).

Our deadline is Monday.

Thanks,

--

Anne Branigin

Staff Writer, The Root

anne.branigin@theroot.com

twitter: [@annebranigin](https://twitter.com/annebranigin)

phone: [\(703\) 624 5040](tel:(703)6245040)

From: Conner, David
Sent: Tuesday, July 10, 2018 11:53 AM
To: '57679-26624274@requests.muckrock.com'
Subject: MPIA 18-0807
Attachments: Policy 604 - Social Media.pdf

Good afternnon Mam,

In reference to your request here is a copy of the current social media policy for the department.

Officer David Conner J211
Baltimore Police Department
Document Compliance Unit
Legal Affairs Division
100 N Holiday St., Room 100,
Baltimore, MD 21202
DCU@baltimorepolice.org
MPIA request forms
<http://law.baltimorecity.gov/office-legal-affairs-baltimore-police-department>

CONFIDENTIALITY NOTICE: The information contained in or attached to this e-mail message may be a privileged and confidential attorney/client communication, or otherwise confidential, and is intended only for the use of the individual or entity to whom it is addressed. If you are not the intended recipient, or the employee or agent responsible for delivering the message to the intended recipient, you are notified that any distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify the Legal Affairs Division immediately by telephone at 410-396-2496 and DELETE the message from your system immediately.

The materials in this e-mail are private and may contain sensitive law enforcement information. Please note that e-mail is not necessarily confidential or secure. Use of e-mail constitutes your acknowledgment of these confidentiality and security limitations. If you are not the intended recipient, be advised that any unauthorized use, disclosure, copying, distribution, or the taking of any action in reliance on the contents of this information is strictly prohibited as covered by the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2521. If you have received this e-mail in error, please immediately notify the sender via telephone or return e-mail.


[Department Access](#) [Inquiry](#)
[NIGP Code Browse](#) | [My Account](#) | [Customer Service](#) | [About](#) | [Current Organization: Baltimore City](#)

November 2, 2015 7:40:17 PM EST



Andrew Jaffee

[Home](#) | [Documents](#)

Open Market Purchase Order P533319

Status: 3PS - Sent

[General](#) | [Items](#) | [Vendor](#) | [Address](#) | [Accounting](#) | [Routing](#) | [Attachments\(4\)](#) | [Notes](#) | [Change Orders](#) | [Reminders](#) | [Summary](#)

Header Information

Purchase Order Number:	P533319	Release Number:	0	Short Description:	Annual Service Agreement
Status:	3PS - Sent	Purchaser:	Kevin Lunsford	Receipt Method:	Quantity
Fiscal Year:	2016	PO Type:	Open Market	Minor Status:	
Organization:	Baltimore City				
Department:	BCPD - POLICE	Location:	PDHQA - BCPD - HQ - ANNEX	Type Code:	
Alternate ID:		Entered Date:	10/29/2015 10:59:38 AM	Control Code:	
Days ARO:	0	Retainage %:	0.00%	Discount %:	0.00%
Required By Date:		Promised Date:		Print Dest Detail:	If Different
Pcard Enabled:	No				
Contact Instructions:	Contact Seble Asmare at (410) 396-2114	Tax Rate:		Actual Cost:	\$18,000.00
Print Format:	PO Print				
Ship-to Address:	ANGELA ALSTON 242 W 29TH STREET BALTIMORE, MD 21211 US Email: angela.alston@baltimorepolice.org Phone: (410)396-2114	Bill-to Address:	BUREAU OF ACCOUNTING & PAYROLL SERVICES 401 E. FAYETTE STREET, 5TH FLOOR BALTIMORE, MD 21202 US Email: City-Payables@BaltimoreCity.gov Phone: (410)396-3745		

PO Header Work Order Number:

Attachments: [General Conditions of Informal Bid or Contract \(04-29-08\).doc](#), [R711951 QUOTE GEOFEEDIA.pdf](#), [R711951 128 5622015A.pdf](#), [Board Letter and Documents 533319.pdf](#)

Primary Vendor Information & PO Terms

Vendor:	00034480 - Geofeedia, Inc.	Preferred Delivery Method:	For City Use Only
Remit-to Address:	Michael Mulroy 820 Davis Street Suite 408 Evanston, IL 60201 US Email: mike@geofeedia.com Phone: (312)257-2925 FAX: (312)508-5535 Id: 36120	Payment Terms:	
		Shipping Terms:	
PO Mailing Address:	Michael Mulroy 820 Davis Street Suite 408 Evanston, IL 60201 US Email: mike@geofeedia.com Phone: (312)257-2925 FAX: (312)508-5535 Id: 36120	Shipping Method:	
		Freight Terms:	

Invoice Information

There are no invoices.

Item Information

Print Sequence # 1.0, Item # 1: Annual service agreement for Geofeedia Professional (Open Source Monitoring) Total of 30 users, up to five(5) Real -Time streams. Administrator functions up to 250,000 posts per month. Maximum search of 15 kilometers. 3PS - Sent

NIGP Code: 208-11
Application Software, Microcomputer

Req # / Item #: R711951 / 1

Receipt Method	Qty	Unit Cost	UOM	Discount %	Total Discount Aml.	Tax Rate	Tax Amount	Freight	Total Cost
Quantity	1.0	\$18,000.00	LOT - Lot	0.00	\$0.00		\$0.00	\$0.00	\$18,000.00

Manufacturer:

Brand:

Model:

Make:

Packaging:

PO Item Work Order
Number:

Account Code	Amount
1001-000000-2041-220100-603026	\$18,000.00

Approval Path:

Delete	Approver	Order Sequence	Approval Path ID	Level	Approver Type	Date Requested	Date Approved/Disapproved	Approved/Disapproved/Canceled by	Comment View
	Christine Parnau	1	MSTERBLKT	10	Primary	10/29/2015 04:59:23 PM	10/29/2015 05:05:15 PM	Christine Parnau	
	Timothy Krus	1	MSTERBLKT	10	Alternative	10/29/2015 04:59:23 PM			
	Sue Ziegler	2		2	Primary	10/29/2015 05:05:17 PM	10/29/2015 05:05:56 PM	Sue Ziegler	

Print

Print Vendor Copy

Copyright © 2015 Periscope Holdings, Inc. - All Rights Reserved. app1



Policy 604

Subject	
SOCIAL MEDIA	
Date Published	Page
1 July 2016	1 of 4

By Order of the Police Commissioner

POLICY

The purpose of this policy is to guide all members of the Baltimore Police Department (BPD) in the professional use of social media, and personal use of social media, only to the extent that personal use of social media sites or platforms may bear on a member's official duties.

1. **Ethical Conduct.** Members have a duty to adhere at all times to BPD's existing standards of conduct, ethics and professionalism. Misconduct of any kind, regardless of whether it occurs on social media, is governed by Policy 301, *Code of Ethics* and Policy 302, *Rules and Regulations*.
2. **Prohibited Uses.** As explained more fully below, members shall not:
 - 2.1. Post privileged or confidential information they have obtained from their employment with BPD.
 - 2.2. Unless authorized, make representations on behalf of the BPD, or give the impression of making a representation on behalf of BPD, on any social media platform.
3. **Importance of Social Media.** BPD recognizes that members have a right to use social media and the significant role that social media can play in members' personal lives. This policy is intended to address only such social media activity that bears on a member's official duties or suggests that the BPD authorizes the posting, or that the member is posting on behalf of the BPD. This policy does not prohibit a member from engaging any social media activity protected by the First Amendment.

DEFINITIONS

Departmental Spokesperson – Any member of the BPD, who has been authorized by the Police Commissioner, his/her designee, or the Director of the Media Relations Section (MRS), to communicate with and/or deliver information to the general public and social/news media on behalf of the BPD.

Member – For the purposes of this policy, the term “member” shall include ALL employees of the BPD, whether sworn, civilian or contractual.

Post – For the purposes of this policy, the term “post” shall be defined, in context, as either: (1) the action of submitting information to the Internet or a social media site; or (2) a collective name for all or part of any information already displayed on the Internet or a social media site.

Social Media – A collective term referring to various online platforms, applications or technologies enabling the “sharing” of electronic, user-generated text, audio, photographic, video or multimedia files.

Social Media Site – A particular application, website or platform that allows social networking,

“blogging,” photograph or video sharing, and similar online activities. (Including but not limited to Facebook, LinkedIn, Twitter, Instagram, YouTube, Reddit, Tumblr, etc.)

MEMBERS’ PERSONAL USE OF SOCIAL MEDIA

1. Members have a right to express themselves as private citizens on social media sites, however, members should not:
 - 1.1. Make, share, or comment in support of any posting that includes criminal conduct, threats of violence or otherwise violates any law.
 - 1.2. Make, share, or comment in support of any posting disparaging of any race, religion, sex, gender, sexual orientation, nationality, or any other protected class of individuals.
 - 1.3. Post, transmit or otherwise disseminate any information, videos or images, in any format that violates Policy 601, *Member Confidentiality Obligations and Media Releases*, which governs every BPD employee’s confidentiality obligations.
 - 1.4. Unless authorized, make any representations on behalf of the BPD.
 - 1.5. Post, transmit or otherwise disseminate any information on personal social media sites while on duty, without permission from a supervisor.
2. For member safety, it is recommended that sworn members do not disclose or allude to their status as BPD members on social media.
 - 2.1. Because of the likelihood that material posted to a social media site will be permanently archived, the disclosure of any information that identifies a member as a BPD employee can endanger member safety and/or limit an officer’s ability to serve in certain undercover or sensitive assignments.
3. Members are cautioned that they should not assume any expectation of privacy when posting information to the Internet or a social media site, regardless of user privacy settings or other access controls.
4. If a member reveals (intentionally or otherwise) his/her employment/position with the BPD, when posting personal comments or material on a social media site:
 - 4.1. The member shall not represent himself/herself as a BPD spokesperson; and
 - 4.2. The member shall make clear that his/her opinions, material and/or comments are not an official statement from the BPD.

NOTE: See Policy 1729, *Whistleblower Protection* for protected member speech.

5. Members should refrain from revealing, in any manner or for any reason, that any other member (e.g., a supervisor, partner, co-worker, etc.) is an employee of the BPD without the express written consent of that other member.
6. Members are personally responsible for any content they “like,” publish, forward or post to the Internet and/or a social media site.

7. Members shall not create or maintain a BPD social media site, unless directly authorized to do so by the Police Commissioner.
8. Members shall not knowingly engage in any type of social media contact (e.g., “friending,” “following,” etc.) that would hamper, interfere with or otherwise prejudice an open or ongoing investigation, case, or court action.
9. Members shall not use a BPD email address to register with or join a social media site.

BPD SOCIAL MEDIA

1. Only the Police Commissioner, his/her designee, the MRS Director, or a designated departmental spokesperson may post, comment or reply on a social media site on behalf of the Baltimore Police Department.
2. BPD will clearly identify its official social media accounts. Where possible, BPD social media accounts shall prominently display the following information and/or statements:
 - 2.1. BPD contact information and a link to the BPD website.
 - 2.2. That pages are maintained by BPD.
 - 2.3. That the opinions expressed by visitors to BPD pages do not reflect the opinions of the BPD.
 - 2.4. That posted comments will be monitored and that BPD reserves the right to remove comments at its discretion such as obscenities, off-topic comments, personal attacks, any comments that jeopardize an ongoing investigation or prosecution, or that otherwise impair BPD’s ability to provide effective law enforcement services to the community.
 - 2.5. That any content posted or submitted for posting is subject to public disclosure.
3. Departmental spokespersons shall not comment on subject matters:
 - 3.1. Beyond their area of professional expertise; or
 - 3.2. On which they are not authorized to represent the BPD.
4. When authorized members – the Police Commissioner, his/her designee, the MRS Director, or a designated departmental spokesperson – represent the BPD on a social media site, they will:
 - 4.1. Use only an approved/official account or user name.
 - 4.2. Adhere to the “Terms of Use Agreement” that governs users’ activity on the site.
 - 4.3. Ensure their status as a representative of the BPD is clearly evident.
 - 4.4. Limit interaction and comments to information within the public domain.
 - 4.5. Not release any information that may in any way be considered confidential.
 - 4.6. Ensure that all content, posted to a social media site on behalf of the BPD, is accurate

and in compliance with BPD policy.

5. The MRS Director shall review and approve all activity involving the BPD's official Internet website(s).
6. If an official BPD social media site or Internet website hosts a public discussion "forum," messaging board, or other interactive commenting feature, the MRS Director shall ensure that:
 - 6.1. A site moderation policy is clearly stated;
 - 6.2. Comments posted by the general public are monitored by a member of the MRS for inappropriate or offensive content; and
 - 6.3. Comments, deemed to be inappropriate or offensive, are removed/deleted from the site.
7. The MRS Director shall coordinate any release of suspect, witness or person-of-interest information with the Chief, Criminal Investigation Division, or his/her designee.
8. The Chief of the Criminal Investigation Division shall consult with the Director of the MRS when there is a belief that an ongoing investigation or intelligence collection effort would benefit from the use of social media. It may be appropriate for members to use non-official BPD social media accounts in the course of a legitimate criminal investigation, or in the course of intelligence collection efforts, related to public safety or potential criminal activity.
 - 8.1. Investigative units may use non-official BPD social media accounts for investigative purposes with written permission of the Police Commissioner.
 - 8.2. These investigative units will maintain a log of all social media postings to non-official BPD accounts.
 - 8.3. Acceptable uses of non-official BPD social media accounts for legitimate law enforcement purposes includes a member creating and/or using a fictitious social media account, user profile, avatar or similar form of online identification.

ASSOCIATED POLICIES

Policy 301,	<i>Code of Ethics</i>
Policy 302,	<i>Rules and Regulations</i>
Policy 305,	<i>Department Values, Vision and Mission</i>
Policy 308,	<i>General Disciplinary Process</i>
Policy 601,	<i>Member Confidentiality Obligations and Media Releases</i>
Policy 602,	<i>Public Speech</i>
Policy 1306,	<i>BPDnet and Internet Usage Policy</i>
Policy 1307,	<i>Personal Communications Devices</i>

RESCISSION

Remove and destroy/recycle Policy 604, *Social Media Policy* dated 12 November 2015.

COMMUNICATION OF POLICY

This policy is effective on the date listed herein. Commanders are responsible for informing their subordinates of this policy and ensuring compliance.



Policy 604

Subject SOCIAL MEDIA	
Date Published 1 July 2016	Page 1 of 4

By Order of the Police Commissioner

POLICY

The purpose of this policy is to guide all members of the Baltimore Police Department (BPD) in the professional use of social media, and personal use of social media, only to the extent that personal use of social media sites or platforms may bear on a member's official duties.

1. **Ethical Conduct.** Members have a duty to adhere at all times to BPD's existing standards of conduct, ethics and professionalism. Misconduct of any kind, regardless of whether it occurs on social media, is governed by Policy 301, *Code of Ethics* and Policy 302, *Rules and Regulations*.
2. **Prohibited Uses.** As explained more fully below, members shall not:
 - 2.1. Post privileged or confidential information they have obtained from their employment with BPD.
 - 2.2. Unless authorized, make representations on behalf of the BPD, or give the impression of making a representation on behalf of BPD, on any social media platform.
3. **Importance of Social Media.** BPD recognizes that members have a right to use social media and the significant role that social media can play in members' personal lives. This policy is intended to address only such social media activity that bears on a member's official duties or suggests that the BPD authorizes the posting, or that the member is posting on behalf of the BPD. This policy does not prohibit a member from engaging any social media activity protected by the First Amendment.

DEFINITIONS

Departmental Spokesperson – Any member of the BPD, who has been authorized by the Police Commissioner, his/her designee, or the Director of the Media Relations Section (MRS), to communicate with and/or deliver information to the general public and social/news media on behalf of the BPD.

Member – For the purposes of this policy, the term "member" shall include ALL employees of the BPD, whether sworn, civilian or contractual.

Post – For the purposes of this policy, the term "post" shall be defined, in context, as either: (1) the action of submitting information to the Internet or a social media site; or (2) a collective name for all or part of any information already displayed on the Internet or a social media site.

Social Media – A collective term referring to various online platforms, applications or technologies enabling the "sharing" of electronic, user-generated text, audio, photographic, video or multimedia files.

Social Media Site – A particular application, website or platform that allows social networking,

“blogging,” photograph or video sharing, and similar online activities. (Including but not limited to Facebook, LinkedIn, Twitter, Instagram, YouTube, Reddit, Tumblr, etc.)

MEMBERS’ PERSONAL USE OF SOCIAL MEDIA

1. Members have a right to express themselves as private citizens on social media sites, however, members should not:
 - 1.1. Make, share, or comment in support of any posting that includes criminal conduct, threats of violence or otherwise violates any law.
 - 1.2. Make, share, or comment in support of any posting disparaging of any race, religion, sex, gender, sexual orientation, nationality, or any other protected class of individuals.
 - 1.3. Post, transmit or otherwise disseminate any information, videos or images, in any format that violates Policy 601, *Member Confidentiality Obligations and Media Releases*, which governs every BPD employee’s confidentiality obligations.
 - 1.4. Unless authorized, make any representations on behalf of the BPD.
 - 1.5. Post, transmit or otherwise disseminate any information on personal social media sites while on duty, without permission from a supervisor.
2. For member safety, it is recommended that sworn members do not disclose or allude to their status as BPD members on social media.
 - 2.1. Because of the likelihood that material posted to a social media site will be permanently archived, the disclosure of any information that identifies a member as a BPD employee can endanger member safety and/or limit an officer’s ability to serve in certain undercover or sensitive assignments.
3. Members are cautioned that they should not assume any expectation of privacy when posting information to the Internet or a social media site, regardless of user privacy settings or other access controls.
4. If a member reveals (intentionally or otherwise) his/her employment/position with the BPD, when posting personal comments or material on a social media site:
 - 4.1. The member shall not represent himself/herself as a BPD spokesperson; and
 - 4.2. The member shall make clear that his/her opinions, material and/or comments are not an official statement from the BPD.

NOTE: See Policy 1729, *Whistleblower Protection* for protected member speech.

5. Members should refrain from revealing, in any manner or for any reason, that any other member (e.g., a supervisor, partner, co-worker, etc.) is an employee of the BPD without the express written consent of that other member.
6. Members are personally responsible for any content they “like,” publish, forward or post to the Internet and/or a social media site.

7. Members shall not create or maintain a BPD social media site, unless directly authorized to do so by the Police Commissioner.
8. Members shall not knowingly engage in any type of social media contact (e.g., “friending,” “following,” etc.) that would hamper, interfere with or otherwise prejudice an open or ongoing investigation, case, or court action.
9. Members shall not use a BPD email address to register with or join a social media site.

BPD SOCIAL MEDIA

1. Only the Police Commissioner, his/her designee, the MRS Director, or a designated departmental spokesperson may post, comment or reply on a social media site on behalf of the Baltimore Police Department.
2. BPD will clearly identify its official social media accounts. Where possible, BPD social media accounts shall prominently display the following information and/or statements:
 - 2.1. BPD contact information and a link to the BPD website.
 - 2.2. That pages are maintained by BPD.
 - 2.3. That the opinions expressed by visitors to BPD pages do not reflect the opinions of the BPD.
 - 2.4. That posted comments will be monitored and that BPD reserves the right to remove comments at its discretion such as obscenities, off-topic comments, personal attacks, any comments that jeopardize an ongoing investigation or prosecution, or that otherwise impair BPD’s ability to provide effective law enforcement services to the community.
 - 2.5. That any content posted or submitted for posting is subject to public disclosure.
3. Departmental spokespersons shall not comment on subject matters:
 - 3.1. Beyond their area of professional expertise; or
 - 3.2. On which they are not authorized to represent the BPD.
4. When authorized members – the Police Commissioner, his/her designee, the MRS Director, or a designated departmental spokesperson – represent the BPD on a social media site, they will:
 - 4.1. Use only an approved/official account or user name.
 - 4.2. Adhere to the “Terms of Use Agreement” that governs users’ activity on the site.
 - 4.3. Ensure their status as a representative of the BPD is clearly evident.
 - 4.4. Limit interaction and comments to information within the public domain.
 - 4.5. Not release any information that may in any way be considered confidential.
 - 4.6. Ensure that all content, posted to a social media site on behalf of the BPD, is accurate

and in compliance with BPD policy.

5. The MRS Director shall review and approve all activity involving the BPD's official Internet website(s).
6. If an official BPD social media site or Internet website hosts a public discussion "forum," messaging board, or other interactive commenting feature, the MRS Director shall ensure that:
 - 6.1. A site moderation policy is clearly stated;
 - 6.2. Comments posted by the general public are monitored by a member of the MRS for inappropriate or offensive content; and
 - 6.3. Comments, deemed to be inappropriate or offensive, are removed/deleted from the site.
7. The MRS Director shall coordinate any release of suspect, witness or person-of-interest information with the Chief, Criminal Investigation Division, or his/her designee.
8. The Chief of the Criminal Investigation Division shall consult with the Director of the MRS when there is a belief that an ongoing investigation or intelligence collection effort would benefit from the use of social media. It may be appropriate for members to use non-official BPD social media accounts in the course of a legitimate criminal investigation, or in the course of intelligence collection efforts, related to public safety or potential criminal activity.
 - 8.1. Investigative units may use non-official BPD social media accounts for investigative purposes with written permission of the Police Commissioner.
 - 8.2. These investigative units will maintain a log of all social media postings to non-official BPD accounts.
 - 8.3. Acceptable uses of non-official BPD social media accounts for legitimate law enforcement purposes includes a member creating and/or using a fictitious social media account, user profile, avatar or similar form of online identification.

ASSOCIATED POLICIES

Policy 301,	<i>Code of Ethics</i>
Policy 302,	<i>Rules and Regulations</i>
Policy 305,	<i>Department Values, Vision and Mission</i>
Policy 308,	<i>General Disciplinary Process</i>
Policy 601,	<i>Member Confidentiality Obligations and Media Releases</i>
Policy 602,	<i>Public Speech</i>
Policy 1306,	<i>BPDnet and Internet Usage Policy</i>
Policy 1307,	<i>Personal Communications Devices</i>

RESCISSION

Remove and destroy/recycle Policy 604, *Social Media Policy* dated 12 November 2015.

COMMUNICATION OF POLICY

This policy is effective on the date listed herein. Commanders are responsible for informing their subordinates of this policy and ensuring compliance.



Policy 801

Subject

OVERDOSE RESPONSE AND INVESTIGATION PROTOCOL

Date Published

23 September 2016

Page

1 of 5

By Order of the Police Commissioner

POLICY

1. **Sanctity of Human Life.** The policy of the Baltimore Police Department (BPD) is to value and preserve human life in all situations.
2. **Overdose Investigations.** Opioid-related overdose fatalities in Maryland increased by 106% between 2011 and 2015, and are expected to continue to rise¹. The BPD shall thoroughly investigate overdose cases to ascertain the source of supply for the chemical substance and assign criminal culpability where appropriate.
3. **Maryland Good Samaritan Law.** A person who, in good faith, seeks, provides, or assists with the provision of medical assistance for a person experiencing a medical emergency after ingesting or using alcohol or drugs shall be immune from criminal prosecution for a violation of 5-601, 5-619, 5-620, 10-114, 10-116, and 10-117 of the Criminal Law Article if the evidence for the criminal prosecution was obtained solely as a result of the person's seeking, providing, or assisting with the provision of medical assistance. Additionally, a person who reasonably believes that they are experiencing a medical emergency after ingesting or using alcohol or drugs shall be immune from criminal arrest, charge, or prosecution for violation of the above statutes if the evidence for the criminal arrest, charge, or prosecution was obtained solely as a result of the person seeking or receiving medical assistance.

REQUIRED ACTION

Non-Fatal Overdose

Patrol Response

1. Render/request medical aid for the victim.
2. If opioid overdose is suspected, administer Naloxone® if trained to do so (See Policy 821, *Use of Naloxone/Narcan for Opioid Overdoses*.)
3. Locate and identify all persons on scene.
4. Obtain initial factual information from all individuals involved/on scene. Be mindful that family members and associates can provide valuable information about the victim's history of

¹ Maryland Department of Health and Mental Hygiene – Overdose Death Report, June 2016.

Policy 801	OVERDOSE RESPONSE AND INVESTIGATION PROTOCOL	Page 2 of 5
-------------------	---	--------------------

addiction/drug abuse as well as possible suppliers and locations where the victim may have purchased the illegal substance.

5. Treat the location as a potential crime scene. Establish a crime scene log, when necessary.
6. Obtain the cell phone and home phone numbers of the victim. Attempt to gain consent to view the cell phone for any text messaging, photographs, or phone numbers that may be related to the source of supply for the overdose substance.

NOTE: Members issued a BWC shall memorialize the attempt to gain consent, as well as record the viewing of the contents of the cell phone into the BWC.

7. Process the scene. This shall include photographing evidence, if necessary, with a BPD-issued digital camera or mobile device.
 - 7.1. In cases of prescription overdose, photograph prescription pill bottles.
8. Secure and submit all evidence. This may include:
 - 8.1. Any suspected controlled dangerous substances or chemical agents believed to have been ingested by the victim.
 - 8.2. Drug paraphernalia (e.g., hypodermic syringe, gelatin capsules, spoon, aluminum foil, glass pipe, etc.).
 - 8.3. CCTV footage.
9. Complete/submit a Crime Incident Report, titled "Overdose," before the end of your tour of duty. The report must contain the following information:
 - 9.1. Victim, witness and/or suspect name, address, date of birth, telephone numbers, and additional pertinent identifying information.
 - 9.2. Detailed crime scene description to include all items of evidence recovered.

NOTE: Include any monikers or identifying markings/characteristics on paraphernalia (e.g., symbols, stars, words/names, colored capsules, etc.) as this may assist investigators with identifying where and from whom the substance was purchased.

- 9.3. Identity of all persons on scene and information they provided.
- 9.4. In cases of prescription overdose (or state if the information is not available):
 - 9.4.1. Medication type, dosage, date prescription was issued, and physician's name.
 - 9.4.2. Name of the pharmacy identified on the prescription container.
 - 9.4.3. Pharmacy prescription number.
 - 9.4.4. Name and address of patient on the label.

Policy 801	OVERDOSE RESPONSE AND INVESTIGATION PROTOCOL	Page 3 of 5
-------------------	---	--------------------

9.4.5. Number of tablets/capsules the victim ingested and remaining pill count.

9.4.6. Reason for the medication.

9.5. In cases involving other chemical agents, attempt to identify the substance and its source, and include such information in the Crime Incident Report.

9.6. Name of hospital where the victim was transported (when applicable).

9.7. Information related to the possible source of supply for the overdose substance, obtained through a lawful search of the cell phone, such as:

9.7.1. Phone numbers.

9.7.2. Contact names.

9.7.3. Text messages.

9.7.4. Photographs/videos.

9.7.5. Social media information.

10. Complete/submit a Heroin/Opioid Overdose Report (See Appendix A).

Patrol Supervisor

1. Respond to the scene of the call.
2. Ensure the scene has been processed and all evidence submitted to the Evidence Control Unit (ECU).
3. Ensure all reports have been submitted and are complete and accurate.
4. Scan and email the Heroin/Opioid Overdose Report (see Appendix A), the Crime Incident Report, and any photographs, property receipts, etc. to Overdose@Baltimorepolice.org.

Fatal Overdose

Patrol Response

1. Notify a permanent-rank supervisor to respond to the scene.
2. Notify the Homicide Section.
3. Be guided by the Homicide Section primary investigator for further investigatory actions/reporting.
4. Seize/submit all cellular telephones or mobile devices belonging to the victim or suspects.

Policy 801	OVERDOSE RESPONSE AND INVESTIGATION PROTOCOL	Page 4 of 5
-------------------	---	--------------------

Patrol Supervisor

1. Respond to the scene of the call.
2. Ensure the scene has been processed and all evidence submitted to the Evidence Control Unit (ECU).
3. Ensure all reports have been submitted and are complete and accurate.
4. Scan and email the Heroin/Opioid Overdose Report (see Appendix A), the Crime Incident Report, and any photographs, property receipts, etc. to Overdose@Baltimorepolice.org.

Crime Scene Unit

1. Respond and process the scenes of all suspected overdose deaths as requested by the Homicide Section.
2. Ensure photographs are loaded to the VeriPic system within the Crime Scene Sciences/Evidence Section.

Homicide Unit

1. Determine if a response to a suspected overdose death is warranted.
2. Direct all investigatory actions of suspected overdose deaths.

Homeland Security Section / Cyber Crimes Unit

1. Assist with the downloading of cellular/mobile device data when requested.
2. Review/collect all overdose reporting.
3. Analyze trends and assign cases for follow-up investigation.

APPENDIX

- A. Heroin/Opioid Overdose Report

ASSOCIATED POLICIES

Policy 703, *Death and Serious Assault Investigations*
Policy 821, *Use of Naloxone/Narcan For Opioid Drug Overdoses*
Policy 1401, *Control of Property and Evidence*
Policy 1402, *Management of Evidentiary CDS*

COMMUNICATION OF POLICY

This policy is effective on the date listed herein. Each employee is responsible for complying with the contents of this policy.

APPENDIX A

Heroin/Opioid Overdose Report

**DEA – W/B HIDTA
Heroin/Opioid Overdose Report**

Responding Officer Agency: _____ County: _____

Incident/Case Number: _____

Incident Date/Time: ____/____/____ ____/____ Fatal Nonfatal (circle one)
mm/dd/yyyy 24:00

Incident Location: _____

Street Number, Street Name, Direction, Apt.

Incident City: _____, MD Incident County: _____

Victim Name: _____

Last First M.I.
Victim DOB: ____/____/____ Victim Gender (circle): M F
mm/dd/yyyyVictim Phone # _____ ☐ Phone Seized ☐ Consent to Search Phone

Home Address: _____, MD

Street Number, Street Name, Direction, Apt

Incident County: _____

Suspect Name: _____ Gender: M F

Last First
Suspect DOB: ____/____/____ Suspect Phone #: _____
mm/dd/yyyy**Suspected Overdose Drug:** ☐ Heroin ☐ Fentanyl ☐ Prescription Drugs ☐ Other (check all that apply)
☐ Packaging found at Scene ☐ CDS Recovered**Naloxone Administered:** ☐ None ☐ 1 dose ☐ 2 doses+ **Responded to Naloxone:** ☐ Yes ☐ No

PROPERTY DIVISION
REQUISITION FOR SUPPLIES
02/128

Police Department
Baltimore, Maryland

Req. # 268796

DISTRICT, DIVISION OR BUREAU: HSS DATE 9/30/2016 PHONE # 410-396-2640

Quantity	COMMODITY	Quantity on Hand	FILLED		
			From Stock	Order Number	Quantity
1	Annual service agreement for Geofeedia Public Safety Edition (open source monitoring). Total of 30 users, with real-time streams and admin. functions. - Unlimited data consumption - Maximum search radius of 15 kilometers - Image Analysis with up to 400,000 images per month within 20 location based recordings	+			
	COMMODITY SOURCE: 820 Davis St, Suite 408 LOCATION: Evanston, IL 60201 JUSTIFICATION: Open source monitoring, location-based software	+			

I HEREBY CERTIFY THAT THE ABOVE ITEMS ARE NECESSARY TO MEET CURRENT NEEDS:

Signature

Print / Type Name

William MacDonald

Signature of Commanding Officer

OK. a per
9/30/16

Bureau of Purchases

JUSTIFICATION FORM

APPENDIX 2

Date: 30 September 2016

Requisition No.: 268796

Agency: Baltimore Police Department

Contact/Phone: 410-396-2640

Vendor: Geofeedia, Inc

Cost: \$ 23,000

Proposes to procure as (select category):

☐ Urgency Justification ☐ Sole Source Justification ☒ Selected Source Justification ☐ Emergency

Proposes to Procure: Software program used to identify actionable intelligence from numerous social media outlets.

Justification: The Homeland Security Section has been using Geofeedia's location-based social media monitoring software for the past three years. Custom interfaces have been developed with other software programs used by the BPD. To replace the software would cause the agency additional expense to recreate the current interfaces. New software would also require training, resulting additional and unnecessary overtime costs to backfill positions.

Urgency Justification (Telephone Quotes) (Check Applicable Box(es))

- ☐ Urgency needed.
☐ Not practicable to obtain through normal channels.
☐ Does not qualify as an emergency purchase.

Sole Source Purchase (Check Applicable Box(es)):

- ☐ Compatibility of equipment, accessories
☐ Or replacement parts is paramount consideration.
☐ Item needed for trial use or testing.
☐ Item being procured for resale.
☐ Public utility being procured.

Selected Source Purchases (Check Applicable Box(es)):

- ☒ No advantage to seeking competition.
☒ Not practicable to obtain competition.
☐ Items are an emergency nature.

Emergency Purchase (Check Applicable Box(es)):

- ☐ Threatens functioning of City government.
☐ Preservation of protection of property.
☐ Health, safety, and welfare of personnel.

I recommend that competitive procurement be waived, and that the supplies, materials, equipment, services, or public works be procured as indicated above.

Signed: 
Agency Head or Designee

Buyer's recommendation:

☐ Approve

☐ Disapprove

Signed: _____

City Purchasing Agent and/or Purchasing Services Supervisor: ☐ Approve ☐ Disapprove

Signed: _____

Order Information

Account Name: Baltimore Police Department
Prepared By: Jon Newman & Jackie Pecirno
Preparation Date: September 30, 2016

Contract Start Date: Upon Signature
Contract End Date: 1 year from start date

Total Amount: \$23,000.00

Subscription Term, Billing & Payment Information

Company Name: Baltimore Police Department
Billing Name: Sgt. William MacDonald
Billing Email: William.macdonald@baltimorepolice.org
Billing Address: 242 W. 29th St.
Baltimore, MD 21211-2908

Billing Phone: (410) 396-2640

Billing Fax:

Payment Method: Invoice

PO Number: _____

Billing Terms: Invoices sent *Upfront*

Payment Terms: Due Upon Receipt. Interest accrues at the rate of 1.5% per month 60 days after the invoice date.
Invoices 30 days or more past due may result in suspension of Services.

This Order Form is subject to and governed by the terms and conditions of the Geofeedia Service Agreement posted online at <http://www.geofeedia.com/legal/service-agreement/> (unless there is already a Geofeedia Service Agreement in force and effect between you and Geofeedia, in which case the terms of such existing Geofeedia Service Agreement shall govern this Order Form). If for any reason you are unable to view the Geofeedia Service Agreement online at <http://www.geofeedia.com/legal/service-agreement/>, please contact Geofeedia immediately.

This Order Form is valid for 30 days from the Preparation Date.

Customer: Baltimore Police Department

Geofeedia, Inc.

Signature: _____

Signature: _____

Printed: _____

Printed: _____

Title: _____

Title: _____

Date: _____

Date: _____

OPTION SELECTED: _____

Order Form (Cont'd) – Baltimore Police Department

Application Services Subscription*

The Application Services include the following:

Service Edition

Total Price

Standard Service Package

Customer orders the following Standard Package:

\$23,000.00

Geofeedia Public Safety Edition

Total Permitted Users: Watch Center – Up to thirty (30)

Search

- Real-Time Search Plus
- Keyword Search
- Discovery Search
- Streamer
- Influencer Search

Engage & Share

- Alerts with Boolean Exclusions
- Notification Inbox
- One-Click Instagram Map Widget
- iOS/Android Mobile App

Archive & Analyze

- Unlimited Data
- Unlimited Recordings
- Analytics
- Translate
- Collections
- CSV Export
- Image Analysis (up to 400,000 images per month within twenty (20) Location Recordings)

Search Radius

- Maximum of 15 kilometers

Support & Services

Included

Unlimited Tutorials & Documentation

Customer Support

Customer Success Manager

Live Webinar Training

Shape File Support

Live Event Monitoring Support & Assistance – includes Super Bowl and other large events

ESRI integration - TBD

Enablement & Training

Optional

Remote

Included

Total Cost

\$ 23,000.00

Order Comments


**NOTE: Please identify which option customer intends to purchase

For additional details regarding standard features and functionality of the Application Services, please visit:

<http://geofeedia.com/how-it-works>

**POLICE DEPARTMENT
BALTIMORE, MARYLAND**

29 September 2016

TO: Major Byron Conaway
VIA: Official Channels 
FROM: Joseph Orenstein
SUBJECT: Justification Letter for Renewal of Geofeedia

Sir,

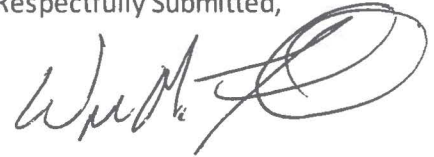
I respectfully request, the Baltimore Police Department renew the location-based social media monitoring platform from Geofeedia. The Homeland Security Section has been using this software platform for the last three years, allowing the department to extract timely and actionable intelligence from vast volumes of social media content that is both geotagged with precise locations using latitude and longitude coordinates and non-geotagged with keyword searches. Geofeedia was selected over other social media data mining platforms due to;

- Data from twelve total sources and non-geotagged sources
- Real-time social content obtained from multiple locations simultaneously
- Ease of data export in various formats into other Baltimore Police Departments databases and software, including ArcGIS and, in the near future, ERSI
- Incorporated sentiment analysis that aids in determining positive versus negative posts
- A cloud-based data center that enables users to store all social data from defined locations if needed
- User friendly network analysis to describe social media relationships, once a subject or target has been identified
- Simple creation of collection ideas for workflow and curation processes
- Embeddable Instagram maps to display content
- Direct import of shape files
- Image recognition and analysis capabilities
- Mobile app on both iOS and Android mobile devices
- Ability to be alerted via email for benchmark and threshold alerts based on where social activity is occurring, number of posters, user activity, sentiment increases, decreases, relative to historical average
- Search, filter, and alert by "emojis"

- Ability to view live streaming social media information for up to 5 separate locations on one screen
- Non-social data overlays which include traffic, weather, and most importantly crisis and natural disaster which can explore real time crisis and natural disasters such as earthquakes, explosions, terror attacks, power outages, etc. in the world next to social data.

While there are other social media monitoring platforms on the market, only Geofeedia meets or exceeds the needs of the Homeland Security Section. The purchase of a new social media monitoring platform would also incur the cost of retraining the operators on the new software and the interfacing with the departments various data and analytic software programs. I therefore request, that Geofeedia be renewed / awarded this purchase order.

Respectfully Submitted,

A handwritten signature in black ink, appearing to read 'Joseph Orenstein', with a large, stylized circular flourish at the end.

Joseph Orenstein

Case Number	Date Received	Date Occurred	Needle Officer(s)	Allegation(s)/Offense Type(s)	Summary	Bureau	Category	Flag	CC # & C. #	Incident Type	Dis. Dt.	Completed Dt.	Incl. Dt.
Withheld Article ("GP"), § 4-311(a)	21-Jan-17	29-Jan-17	Withheld Article ("GP"), § 4-311(a)	Conduct Unbecoming a Police Officer/Employee - Disposition Withheld Article ("GP"), § 4-311(a) Conduct Unbecoming a Police Officer/Employee - Disposition Withheld Article ("GP"), § 4-311(a) Conduct Unbecoming a Police Officer/Employee - Disposition Withheld Article ("GP"), § 4-311(a) Conduct Unbecoming a Police Officer/Employee - Disposition Withheld Article ("GP"), § 4-311(a) Conduct Unbecoming a Police Officer/Employee - Disposition Withheld Article ("GP"), § 4-311(a) Conduct Unbecoming a Police Officer/Employee - Disposition Withheld Article ("GP"), § 4-311(a)	Withheld Article ("GP"), § 4-311(a)	Operational			CC # E. C. #181100001	Ethics	1-May-17	21-Jun-17	21-Jun-17
Withheld Article ("GP"), § 4-311(a)	15-Nov-17		Withheld Article ("GP"), § 4-311(a)	Conduct Unbecoming a Police Officer/Employee - Disposition Withheld Article ("GP"), § 4-311(a) Inappropriate Comments and/or Gestures - Disposition Withheld Article ("GP"), § 4-311(a)	Withheld Article ("GP"), § 4-311(a)	Operational				External Complaints	14-Jun-17	10-Oct-17	10-Oct-17
Withheld Article ("GP"), § 4-311(a)	12-Nov-18	11-Nov-18	Withheld Article ("GP"), § 4-311(a)	Conduct Unbecoming a Police Officer/Employee - Disposition Withheld Article ("GP"), § 4-311(a) Computer/Email/Internet Misuse - Disposition Withheld Article ("GP"), § 4-311(a) You/Other Misdeemeanor - Disposition Withheld Article ("GP"), § 4-311(a)	Withheld Article ("GP"), § 4-311(a)	Operational				External Complaints	10-Feb-19	17-Sep-19	17-Sep-19
Withheld Article ("GP"), § 4-311(a)	23-Apr-19		Withheld Article ("GP"), § 4-311(a)	Conduct Unbecoming a Police Officer/Employee - Disposition Withheld Article ("GP"), § 4-311(a) Computer/Email/Internet Misuse - Disposition Withheld Article ("GP"), § 4-311(a) Harassment - Disposition Withheld Article ("GP"), § 4-311(a)	Withheld Article ("GP"), § 4-311(a)	Operational				External Complaints	22-Apr-20	20-Apr-20	20-Apr-20
Withheld Article ("GP"), § 4-311(a)	17-Jan-20	16-Jan-20	Withheld Article ("GP"), § 4-311(a)	Conduct Unbecoming a Police Officer/Employee - Disposition Withheld Article ("GP"), § 4-311(a) Computer/Email/Internet Misuse - Disposition Withheld Article ("GP"), § 4-311(a)	Withheld Article ("GP"), § 4-311(a)					External Complaints	16-Jan-21	16-Feb-20	16-Feb-20