



Nathan Woodliff-Stanley, Executive Director  
Mark Silverstein, Legal Director

October 6, 2016

**SENT VIA EMAIL:** [mary.dulacki@denvergov.org](mailto:mary.dulacki@denvergov.org)

Mary Dulacki  
Director of Records Management  
Denver Department of Safety  
1331 Cherokee Street, Suite 302  
Denver, CO 80204

Dear Mary:

I write to request records pursuant to the Colorado Open Records Act and the Colorado Criminal Justice Records Act.

This request seeks information and records related to the Denver Police Department's acquisition of, and its policy and practice regarding, software designed to access information from social media services.<sup>1</sup>

This request for records is prompted by the Daily Dot's publication of an article about the Denver Police Department's recent purchase of access to Geofeedia. *See* Dell Cameron, The Daily Dot, September 18, 2016, "*Denver police spent \$30K on social media surveillance tools in May,*" available at <http://www.dailydot.com/layer8/denver-police-geofeedia-social-media-monitoring/>. A copy of that article is attached to this letter requesting records.

The following description of the records requested will refer, in places, to this article.

1. Please provide copies of records referencing the purchase of, acquisition of, installation of, subscription to, payment for, or agreements for Geofeedia and any other software designed to access information from social media services.

---

<sup>1</sup> Throughout this request, the term "**software designed to access information from social media services**" includes but is not limited to software that enables the monitoring, searching, collection, or analysis of user-generated content located on social media services. Examples of such software include Geofeedia, MediaSonar, and X1Social Discovery. Examples of such social media services include, but are not limited to, Facebook, Instagram, Twitter, Google Plus, Pinterest, YikYak, Reddit, SnapChat, and MySpace. "Software designed to access information from social media services" does not include a mobile application or website operated by a social media service.

2. Please provide copies of your correspondence with Dell Cameron or The Daily Dot regarding Geofeedia. This request includes:
  - a. A copy of The Daily Dot's request for records;
  - b. A copy of Denver's response to The Daily Dot, including the documents provided to The Daily Dot
3. It is my understanding that the \$30,000 that Denver paid to Geofeedia provided for access for 30 users. Please provide documents that will reveal the name, badge number, and assignment of each Denver Police Department employee who is authorized to access Geofeedia.
4. Please provide copies of all written communications between any employees of the Denver Police Department and the vendors any software designed to access information from social media services, including, but not limited to, Geofeedia.
5. Please provide a copy of the user agreement between the Denver Police Department and Geofeedia.
6. Please provide copies of all materials used in the training of Denver police officers in the use of Geofeedia.
7. Please provide copies of all promotional materials printed or distributed by Geofeedia that are in the possession of, or have been accessed by employees of, the Denver Police Department.
8. Please provide documents that will reveal the number of times that Denver Police Department personnel have accessed Geofeedia since the purchase of access in May, 2016.
9. Please provide documents that will reveal the dates that Denver Police Department personnel have accessed Geofeedia since the purchase of access in May, 2016.
10. Please provide documents that will reveal each of the search terms that Denver Police Department personal have used when accessing Geofeedia at any time since the purchase of access in May, 2016.
11. Please provide any internal memos, reports, or other documents that mention or refer to the Denver Police Department's use of Geofeedia.
12. Within the Denver Police Department, the request to purchase access to Geofeedia was made by the commander of the Denver Police Department's Intelligence Unit. In 2003, Denver entered into a Settlement Agreement to resolve a class action suit, American Friends Service Committee v. City and County of Denver, No. 02-N-0740, United States District Court, District of Colorado. This case, which came to be known as the "Spy Files" case, challenged the Intelligence Unit's practice of monitoring and collecting information on the First Amendment activities of law-abiding activists and advocacy groups. The Settlement Agreement required the Denver Police Department to adopt the

intelligence policy that was attached as Exhibit 1 to that Agreement. The policy was adopted as Policy 118.03, which is titled "Criminal Intelligence Information." Please provide a copy of the latest version of this policy.

13. In addition, please provide me with copies of any other policies, guidelines, memoranda or other documents drafted since May, 2003, that address or discuss the gathering of intelligence information by the Denver Police Department generally, or the Intelligence Unit in particular.

14. Please disclose whether the Denver Police Department has a written policy regarding the monitoring or collection of information from social media, or the use of social media surveillance software such as Geofeedia, for use in investigations or intelligence gathering. If the Denver Police Department has such a policy, please provide a copy.

Pursuant to C.R.S. § 24-72-305.5, I affirm that the requested records will not be used for the direct solicitation of business for pecuniary gain. The ACLU of Colorado is a non-profit organization that seeks the records for a non-commercial public purpose, including non-profit activities, research, and/or journalism. If your office so provides, I request a reduced or waived fee pursuant to C.R.S. § 24-72-205(4).

If the records are in electronic form or can be scanned and sent by email, I ask to receive those records solely by electronic means sent to [msilverstein@aclu-co.org](mailto:msilverstein@aclu-co.org). If the copies cannot be transmitted electronically, and any anticipated charges will be less than \$50.00, please mail the copies to this office with an invoice for copying charges, which will be paid promptly. If the anticipated charges will be more than \$50.00, or if your office requires prepayment for copies, please first contact me at (720) 402-3114. If the estimated charges will be more than \$50.00, I may choose to first inspect the records and then designate a limited subset for copying.

If you deny this request for records in whole or in part, I ask that you provide forthwith a written statement of the reasons for the denial that cites the law or regulation that you rely on. C.R.S. §§ 24-72-204(4) & 24-72-305(6). If any of the requested records are in active use, in storage or otherwise unavailable at this time, I likewise request that you provide forthwith a written statement and that the custodian set a date and hour at which time the records will be available for inspection. C.R.S. §§ 24-72-203(3)(a) & 24-72-303(3).

I look forward to your response to this request for documents at your earliest convenience, and no later than three business days, as required by Colorado law. Thank you in advance for your attention to this matter.

Sincerely,



Mark Silverstein  
Legal Director, ACLU of Colorado

Attachment

## L A Y E R 8

## Denver police spent \$30K on social media surveillance tools in May

Dell Cameron —Sept 19 at 12:58PM | Last updated Sept 19 at 6:19PM



*Photo via Lilac Mountain / Shutterstock.com (Licensed)*

The funding was acquired through civil asset forfeiture, records show



In May, Denver police spent at least \$30,000 on surveillance software designed to monitor and collect social media posts across at least a dozen networks, according to police records.

Documents acquired by Daily Dot under the Colorado Open Records Act include an invoice to the Denver Police Department from Geofeedia, Inc., a startup whose location-based surveillance wares are exhibited at national security and law enforcement summits across the country.

Geofeedia's products—one of a dozen or so nearly identical online tools employed by U.S. law enforcement on a daily basis—include a powerful platform for the interception, aggregation, and storage of online posts across multiple social media networks.

With Geofeedia, Denver police have acquired the ability to simultaneously monitor posts on [Facebook](#), [Twitter](#), [YouTube](#), [Instagram](#), [Vine](#), [Periscope](#), and [Flickr](#), among others. Its location-based search capabilities enable police to vacuum up nearly every social media post emanating from within specified geographical boundaries. The tweets, photos, videos, and live broadcasts of anyone identified by the software within the area are intercepted and recorded by police through a process developers call “geo-fencing.”

Purchase and requisition paperwork for Geofeedia show Denver police purchased 30 subscriptions to the company's platform using \$30,000 in confiscated funds, which was approved by the city's Property Confiscation Board in March. Approval for the use of seized assets in this purchase was approved directly by Denver Police Chief Robert White, records show.

Tools like Geofeedia offer police the ability to conduct real-time social media surveillance during mass shootings or terrorism events. They are also capable of sucking up copious amounts of data about criminals and innocents alike, information which can then be stored by authorities for later use. (Police records cited by the *Baltimore Sun* earlier this month describe how Baltimore police are using Geofeedia to archive social media posts in a secure data warehouse.)

Denver P.D. denied the Daily Dot access to records concerning the types of social media posts it has acquired through Geofeedia's platform, describing the posts as "confidential intelligence information." A request for access to any training materials, or paperwork that would describe the software's functionality, was also denied. According to police, "the proprietary interests of the manufacturer outweighs any public purpose to be served by release" of said records, if they exist. While exempting certain records about social media monitoring from disclosure, Denver P.D. also cited confidential "tactical, strategic, and investigative information."

"In the U.S. we've never had a secret police that circulates around civil society just looking for anybody saying anything suspicious. We shouldn't have an online equivalent either."

A police spokesperson did not respond to a request for comment about Geofeedia or the allocation of confiscated funds used to purchase its platform. In the past, police departments have defended the use of such software, promoting in particular its ability to identify eyewitnesses to crimes who might have otherwise never come forward. It may also be used to locate guns in schools or identify the sources of illegal drug activity.

Jay Stanley, a senior policy analyst at the American Civil Liberty Union (*ACLU*), said that while platforms like Geofeedia have practical uses, the public should be wary of how they are used. "Even though you obviously don't need a warrant to read stuff that's been published for the world to see, that doesn't mean—as a policy matter—it's a good idea for us to give our police license to engage in mass social media monitoring."

Stanley, who works at ACLU's Speech, Privacy, and Technology Project, also warned of the potential "chilling effect" on First Amendment activities "when we realize there might be a law enforcement officer looking over our shoulder as we

post things online. In the U.S. we've never had a secret police that circulates around civil society just looking for anybody saying anything suspicious. We shouldn't have an online equivalent either.”

In addition to Geofeedia actively working to defeat the privacy controls offered to users by sites like Facebook, its current monitoring software is able to correlate data from more than a dozen networks simultaneously. Individually the posts it collects might be garbage, but in aggregate, over a long enough period of time, the data generated by an active social media users begins to paint an intensive portrait of that person’s identity, their interests, habits, and political affiliations; information that, if not entirely misleading, may not be so wittingly surrendered after all.

“There could definitely be a mosaic effect in which different pixels of information about you can be put together into a higher resolution view of your life,” says Stanley. “That’s one reason why people need to be very conscious and aware of what they are posting online, and why, as a policy matter, we should put in place rules that stop police from trawling around in social media without good reason.”

In a statement, Attorney Stephanie Lacambra of the Electronic Frontier Foundation (EFF) described the use of social media monitoring by police departments as “incredibly troubling for the preservation of individual privacy.”

“I often run into the widespread misperception that ‘because I’m not doing anything wrong,’ or ‘I have nothing to hide,’ ‘digital privacy doesn’t concern me,’” Lacambra said. “This perspective is troubling because it fails to grasp the power of information in the digital age and its potential for abuse—by law enforcement and others.”

According to [TechCrunch](#), Geofeedia raised approximately \$17 million in funding at the beginning of the year. While not mentioning its law enforcement ties, the website noted Geofeedia had acquired “200 new customers in 2015” while experiencing “250 percent year-over-year” growth in revenue. The report listed among its private industry clients Dell, CNN, Mall of America, and the NCAA.

Geofeedia did not immediately respond to a request for comment.