

**Congress of the United States**  
**Washington, DC 20515**

May 2, 2017

The Honorable Jeff Sessions  
Attorney General  
U.S. Department of Justice  
950 Pennsylvania Avenue, NW  
Washington, DC 20530

Dear Attorney General Sessions:

We write to inquire about the use of social media monitoring technologies by the federal government and federal law enforcement agencies, as well as funding by the federal government of the use of such technologies by local and state law enforcement agencies.

A 2016 survey of 539 law enforcement agencies in 48 states and the District of Columbia found that nearly three-quarters of the surveyed agencies used social media to conduct intelligence gathering for investigations.<sup>[i]</sup> In another study, 156 state and local jurisdictions spent at least \$10,000 on sophisticated social media monitoring technology. However, only 18 had publicly available policies governing their use for criminal investigations or intelligence gathering.<sup>[ii]</sup> Critically, less is known about the use of these tools by the federal government, in particular by the FBI, the DEA, and other arms of the Department of Justice. Moreover, additional transparency is sorely needed regarding the federal government's guidelines for funding local entities for acquisition of these tools.

Social media information can be utilized by law enforcement in various ways: by directly observing publicly-available information on social media platforms; by using informants or undercover accounts; or by using analytical tools that analyze relationships, infer individuals' locations, track groups, and more. While social media data can be a useful tool for apprehending criminals in cases related to property destruction, human trafficking and homicide, it can also be misused in ways that implicate Americans' rights to free speech and freedom of association, as well as what the Supreme Court has recognized as the evolving Fourth Amendment right to privacy in our digital age.

There is evidence that social media data has been used to monitor protests and activists, disproportionately affecting communities of color. An investigator at the Oregon Department of Justice used a service called DigitalStakeout to search Twitter for tweets using the hashtag #BlackLivesMatter. On the basis of his tweets – which included political cartoons and commentary but no indications of criminal activity or violence – the Department's own Director of Civil Rights was deemed a “threat to public safety.”<sup>[iii]</sup> The investigator was subsequently fired by the Oregon Attorney General after the Director filed a complaint.<sup>[iv]</sup> In Baltimore, after

the death of Freddie Gray, the city's police used a service called Geofeedia to monitor protestors, including high school students who planned a walk-out; some evidence suggests that the online surveillance may itself have contributed to an escalation of the tensions between the community and the police.<sup>[v]</sup>

Notably, the ACLU of Northern California obtained records last fall indicating that Geofeedia had advertised its services for precisely that purpose.<sup>[vi]</sup> Several of the major social media platforms have barred Geofeedia and other similar companies from using their data for surveillance purposes in the wake of these revelations, but this is unlikely to be the last word, given the rapid evolution of technology. In addition, this move does not impact the ability of police departments to monitor social media in more direct ways.<sup>[vii]</sup>

Undercover accounts, for example, may be used to monitor lawful protest activities. The Mall of America, for instance, created undercover Facebook accounts to connect with activists and build dossiers on them; these actions appear to have been undertaken in coordination with the Bloomington, Minn. City Attorney's Office, and with the involvements of an FBI Joint Terrorism Task Force as well.<sup>[viii]</sup> Fusion centers, which were created under the auspices of the Department of Justice and Department of Homeland Security to focus on counterterrorism efforts in the wake of 9/11, have also spent resources observing activists on Twitter and Facebook.<sup>[ix]</sup>

Youth of color are often disproportionately monitored online. Perhaps the most notorious example is that of Jelani Henry, a teenager who was wrongly charged with murder based in large part on having been deemed a criminal affiliate after "liking" friends' videos on Facebook.<sup>[x]</sup> Henry ultimately spent two years on Rikers Island awaiting trial, including nine months in solitary confinement, until his case was dismissed.

In addition, some analytic technologies assign a "threat score" to individuals based on a variety of factors, including the content of their social media posts. This process is not transparent and could result in errors, raising questions about the reliability of the technology, how it is being used by law enforcement agencies, and the mechanisms for oversight and accountability.<sup>[xi]</sup>

Finally, there are concerns that social media monitoring technologies can extrapolate data about users' locations through geotagging and other methods, and can infer large volumes of information about individuals that might otherwise be inaccessible.<sup>[xii]</sup> One company was described as having the ability to "scrape and analyze massive volumes of data from Facebook and Twitter and process it for keywords and geographic locations that reveal 'patterns of interest.'"<sup>[xiii]</sup> These data mining capabilities could run afoul of an individual's right to privacy, in light of the Supreme Court's growing recognition of the Fourth Amendment impact of inexpensive, large-scale surveillance capabilities.<sup>[xiv]</sup>

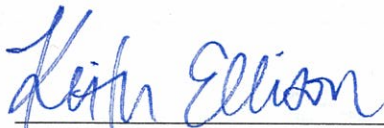
In order to ensure transparency and accountability, we seek answers to the following questions:

- 1) How does the federal government use social media monitoring technology, whether directly monitoring social media platforms, using informants or undercover accounts, or utilizing an analytical software product provided by a third party or developed within an agency? Please detail why this technology is used in each example.

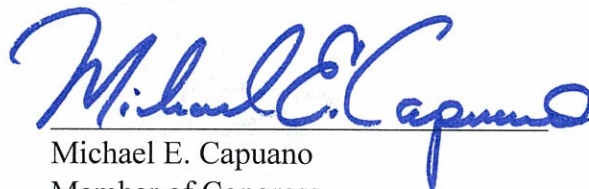
- 2) What measures are in place to protect First Amendment rights, including ensuring that social media monitoring are not used to monitor or track people solely on the basis of the First Amendment-protected speech or associations? This would include monitoring individuals based on a hashtag such as #BlackLivesMatter or inferring the shared location of a group of people who are associating or planning to assemble.
- 3) What measures are in place to protect Fourth Amendment rights, particularly in light of the acknowledgement of a majority of justices in *U.S. v. Jones* and *California v. Riley* that the accumulation and analysis of a quantity of information that previously would have been impossible or prohibitively expensive to collect implicates Constitutional rights to privacy?
- 4) What measures are in place to prevent an undue amount of scrutiny on communities of color, religious minorities, or immigrant and refugee communities?
- 5) How is the use of these technologies audited? How often do audits occur, who is responsible for conducting them, and how is the resulting data used?
- 6) How long does law enforcement store the data collected?
- 7) What training is provided regarding social media monitoring to ensure that social media data is collected and used responsibly and accurately? Does the training, if any, include information about the disproportionate use of social media monitoring against communities of color, the privacy interests implicated by social media monitoring, or the susceptibility of social media postings to misinterpretation?
- 8) What guidelines or standards are in place to guide judgments about when interaction on social media rises to the level of a criminal involvement? Relatedly, what guidelines are in place to ensure that non-criminal social media data collected about an individual is not stored and used for a separate, unrelated crime investigation of the same individual at a later date?
- 9) How much funding has the Department of Justice provided to local and state law enforcement agencies to conduct social media monitoring, either by the agency itself or through the purchase of social media monitoring software? Please break this amount down into the following categories: total annual amount for each year funding has been provided; each agency or entity receiving such funding, the year in which such funding was provided, and the purpose or purposes for which such funding was provided; and copies of any agreements or memoranda of understanding between such agency and the Department of Justice, or the social media monitoring company and the Department of Justice, regarding such funding or purchases.

- 10) What reporting does the Department of Justice require from local or state entities that receive funding to conduct social media monitoring? For instance, does the DOJ require that agencies conduct an analysis of possible discriminatory use or impact of such tools, have auditing procedures in place and provide confirmation that such audits are occurring on a regular basis, or other requirements?
- 11) How much has the Department of Justice spent on technology for the purpose of monitoring, tracking, following, or investigating persons or groups on social media? Please break this amount down into the following categories: total annual amount for each year spending has occurred; the DOJ arm on whose behalf such money has been expended (e.g., FBI, DEA, U.S. Marshal's Office, etc.) in each year; the company, if any, that has received such money; and copies of any relevant contracts or memoranda of understanding between the DOJ and such companies.

Sincerely,



Keith Ellison  
Member of Congress



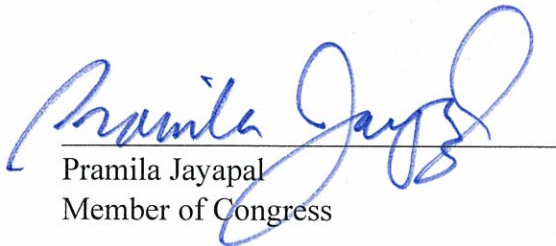
Michael E. Capuano  
Member of Congress



Dwight Evans  
Member of Congress



Raul M. Grijalva  
Member of Congress



Pramila Jayapal  
Member of Congress



Henry C. (Hank) Johnson Jr.  
Member of Congress



Brenda L. Lawrence  
Member of Congress



Barbara Lee  
Member of Congress





Gwen Moore  
Member of Congress



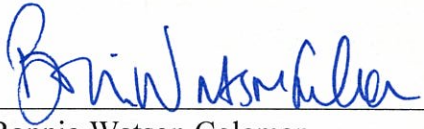
Grace F. Napolitano  
Member of Congress



Jan Schakowsky  
Member of Congress



Mark Takano  
Member of Congress



Bonnie Watson Coleman  
Member of Congress

- 
- <sup>[i]</sup> <http://www.theiacp.org/Portals/0/documents/pdfs/2016-law-enforcement-use-of-social-media-survey.pdf>
- <sup>[ii]</sup> See <https://www.brennancenter.org/analysis/map-social-media-monitoring-police-departments-cities-and-counties>.
- <sup>[iii]</sup> See <http://www.wweek.com/news/2016/04/15/oregon-department-of-justice-civil-rights-chief-intends-to-sue-his-agency-over-black-lives-matter-surveillance/>;  
<https://s3.amazonaws.com/wapopartners.com/wweek-wp/wp-content/uploads/2016/04/15172052/Johnson-complaint.pdf>.
- <sup>[iv]</sup> [http://www.oregonlive.com/politics/index.ssf/2016/10/black\\_lives\\_matter\\_profiling.html](http://www.oregonlive.com/politics/index.ssf/2016/10/black_lives_matter_profiling.html).
- <sup>[v]</sup> <http://www.spin.com/2016/10/social-media-surveillance-probably-played-a-role-in-sparking-the-freddie-gray-riot/>
- <sup>[vi]</sup> [https://medium.com/@ACLU\\_NorCal/police-use-of-social-media-surveillance-software-is-escalating-and-activists-are-in-the-digital-d29d8f89c48#.q206gibzb](https://medium.com/@ACLU_NorCal/police-use-of-social-media-surveillance-software-is-escalating-and-activists-are-in-the-digital-d29d8f89c48#.q206gibzb).
- <sup>[vii]</sup> <https://techcrunch.com/2016/10/11/facebook-twitter-cut-off-data-access-for-geofeedia-a-social-media-surveillance-startup/>.
- <sup>[viii]</sup> <https://theintercept.com/2015/03/18/mall-americas-intelligence-analyst-catfished-black-lives-matter-activists-collect-information/>; <http://www.citypages.com/news/emails-show-city-attorney-colluded-with-mall-of-america-to-prosecute-protesters-6537820>; <https://theintercept.com/2015/03/12/fbi-appeared-use-informant-track-black-lives-matter-protest/>.
- <sup>[ix]</sup> <https://privacysos.org/blog/so-called-counterterror-fusion-center-in-massachusetts-monitored-black-lives-matter-protesters/>.
- <sup>[x]</sup> <http://www.theverge.com/2014/12/10/7341077/nypd-harlem-crews-social-media-rikers-prison>
- <sup>[xi]</sup> [http://www.aclunc.org/docs/201512-social\\_media\\_monitoring\\_software\\_pra\\_response.pdf](http://www.aclunc.org/docs/201512-social_media_monitoring_software_pra_response.pdf);  
[https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c\\_story.html?utm\\_term=.ed0553f1ca7b](https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c_story.html?utm_term=.ed0553f1ca7b).
- <sup>[xii]</sup> See, e.g., <http://www.officer.com/article/12155701/how-to-use-social-media-amidst-protests>
- <sup>[xiii]</sup> <https://www.revealnews.org/article/homeland-security-office-oks-efforts-to-monitor-threats-via-social-media/>.
- <sup>[xiv]</sup> See, e.g., <https://object.cato.org/sites/cato.org/files/serials/files/supreme-court-review/2014/9/pincus.pdf>.