Privacy Impact Assessment Update
for the

Office of Operations Coordination and Planning

Publicly Available Social Media Monitoring and Situational Awareness Initiative

DHS/OPS/PIA-004(f)

May 13, 2015

Contact Point
Carl Gramlick
Director, Operations Coordination Division
Office of Operations Coordination and Planning
(202) 282-8611

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Office of Operations Coordination and Planning (OPS), National Operations Center (NOC) leads the Publicly Available Social Media Monitoring and Situational Awareness Initiative (Initiative). The Initiative assists the Department of Homeland Security and its Components fulfill their statutory responsibility under Section 515 of the Homeland Security Act[1] to provide situational awareness and establish a common operating picture for the Federal Government, and for those state, local, and tribal governments, as appropriate. OPS is updating this Privacy Impact Assessment (PIA) to address the privacy impact of using geospatial information offered by mobile media to enhance situational awareness.

Overview

The Department of Homeland Security (DHS) Office of Operations Coordination and Planning (OPS), which also includes the National Operations Center (NOC), monitors publicly available online forums, blogs, public websites, Twitter, and message boards to collect information to provide situational awareness and establish a common operating picture. In April 2014, the Privacy Office published findings from the sixth Privacy Compliance Review (PCR)[2] of the Initiative. The Privacy Office found that the OPS/NOC uses Global Positioning System (GPS) and geographic location features offered through social media platforms to enhance its search and reporting capabilities. Many mobile applications have built-in functionality that relies on users' location information to provide additional features and services. Major social media platforms allow users to attach location information when making posts (e.g., text, picture, video). With the widespread use of online services and applications on mobile devices that are equipped with GPS, OPS is updating the Initiative PIA to address the privacy impact of the availability of geospatial functions within mobile media to enhance DHS situational awareness.

Reason for the PIA Update

The Privacy Office conducted its sixth PCR of the OPS/NOC Media Monitoring Center (MMC) in coordination with OPS/NOC leadership for the period of March 2013 through December 2013. During the PCR, the Privacy Office found that the OPS/NOC MMC uses geographic filters during crises or major events (e.g., Olympics, Presidential Inaugurations) to limit social media search results to only those that are from a specific geographic location. Using geographic fencing (geofencing)[3] reduces the amount of data that must be analyzed and

[1] 6 U.S.C. § 321d(b)(1).
[2] OPS/NOC MMC PCR #6, *available at* http://www.dhs.gov/sites/default/files/publications/privacy-pcr-media-monitoring-20140416_2.pdf.
[3] Geofencing is a technology that defines a virtual boundary around a real-world geographical area.

significantly enhances the reliability of the information. Geofencing leads to more reliable information than using geographic keywords in searches (e.g., entering "Boston" as a search term) because the filter confirms that the individual providing the information is in the proximity of the location or event of interest. Confirming that information is coming from the scene of an incident provides additional corroboration that an event is occurring, and in some instances, lends a higher degree of credibility to the information itself.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

No change from the April 2013 PIA update. The OPS/NOC MMC does not actively seek or collect personally identifiable information (PII), but the OPS/NOC MMC may collect PII in limited situations.[4]

Characterization of the Information

In traditional searches, internet users can apply geographic keywords (e.g., country, state, county, city, organization, building names) to refine and increase the quality of their search results. Advanced online search platforms have geographic location filtering mechanisms that can use location meta-data (location of the news organization or location of the event) attached to an online article to limit search results to only those that occur in a specific location.

Similarly, OPS/NOC MMC analysts apply geofencing as an additional filter to search social media feeds. OPS/NOC MMC analysts perform geographic location searches using three geographic parameters (latitude, longitude, and radius) of a location of interest. The location of interest defined in a geographic location search is a physical location (e.g., school, university, airport, courthouse) not the location of a specific user.

Privacy Risk: Depending on the size of a search radius, there is a risk that the MMC could inadvertently collect PII.

Mitigation: The OPS/NOC mitigated this risk by establishing effective policies to avoid collection of PII outside the scope of the discrete set of categories discussed in DHS/OPS/PIA-004(e), and to redact that PII if collected inappropriately. The OPS/NOC MMC only monitors

[4] For more information on when the MMC collects PII, see DHS/OPS/PIA-004(e) Publicly Available Social Media Monitoring and Situational Awareness Initiative Update, *available at* www.dhs.gov/privacy.

publicly accessible sites on which users post information voluntarily. Only users who elect to make their location available for public searches will appear in the search results.

Uses of the Information

The OPS/NOC MMC uses geofencing to only receive search results that contain social media postings that are submitted within the defined location, by users who have made their location available for public searches. Geofencing enables MMC analysts to efficiently organize and view returned search results to significantly enhance the reliability of the information by providing a precise location of an event in order to notify the appropriate officials. However, geofencing does not provide a special set of meta-data and no meta-data is collected. The ability to confirm that information is coming from the scene of an incident provides additional corroboration that an event is occurring, and in some instances lends a higher degree of credibility to the information itself.

Notice

DHS provides notice of this increased information collection through this PIA, the Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion SORN, and the Publicly Available Social Media Monitoring and Situational Awareness SORN.[5] Information posted to social media approved for monitoring under the MMC is publicly accessible and voluntarily generated. The social media sites the MMC monitors are public websites. All users have access to their own information through their user accounts. Individuals should consult the privacy policies of the services to which they subscribe for more information.

Data Retention by the project

No change from the April 2013 PIA. The NOC MMC continues to retain information for five years. The NOC MMC is still working with NARA on a retention schedule to immediately delete PII.

Information Sharing

No change from April 2013 PIA Update.

Redress

No change from April 2013 PIA Update.

[5] DHS/OPS-003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion, 75 FR 69689 (Nov. 15, 2010); DHS/OPS-004 Publicly Available Social Media Monitoring and Situational Awareness Initiative, 76 FR 5603 (Feb. 1, 2011).

Auditing and Accountability

Since publishing the first OPS/NOC PIA in June 2010, the DHS Privacy Office conducted six PCRs to assess the OPS/NOC's compliance with the privacy protections described in the PIA.[6] The most recent PCR focused on OPS/NOC's activities from March 2013 to December 2013, and assessed its compliance with both the April 2013 PIA Update and the February 2011 SORN. The DHS Privacy Office found that the OPS/NOC continues to be in compliance with the privacy requirements identified in both of these documents. There are no changes in auditing and accountability from the 2013 PIA Update.

Responsible Official

Carl Gramlick
Director, Operations Coordination Division
Office of Operations Coordination and Planning

Approval Signature

Original signed copy on file with the DHS Privacy Office.

____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

[6] All PCRs related to the OPS/NOC Initiative *available at* http://www.dhs.gov/privacy-investigations-compliance-reviews.