Privacy Impact Assessment
For the

Office of Operations Coordination and Planning

April 2010 BP Oil Spill Response Social Media Event Monitoring Initiative

April 29, 2010

Contact Point
Donald Triner Director (Acting), National Operations Center
Office of Operations Coordination and Planning
(202) 282-8611

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Office of Operations Coordination and Planning (OPS), National Operations Center (NOC), has launched an April 2010 BP Oil Spill Response Social Media Event Monitoring Initiative (Initiative) to assist the Department of Homeland Security (DHS) and its components involved in the security, safety, and emergency response associated with the BP oil spill response off the Gulf Coast. The NOC is using this vehicle to fulfill its statutory responsibility to provide situational awareness and establish a common operating picture for the federal government, and for those state, local, and tribal governments, as appropriate, assisting with the security, safety, and emergency response associated with the oil spill. OPS may also share information with international partners and the private sector where necessary and appropriate for security, safety, and emergency response coordination. The NOC is only monitoring publicly available online forums, blogs, public websites, and message boards to collect information used in providing situational awareness and to establish a common operating picture. OPS will not set up user accounts to access any information. While this Initiative is not designed to collect personally identifiable information (PII), OPS is conducting this Privacy Impact Assessment (PIA) because the Initiative could potentially involve personally identifiable information (PII) or other information received in an identifiable form. This PIA is effective for 60 days and will expire at that time. Should the requirements for the Initiative change before this expiration date, OPS and the Privacy Office will immediately update this PIA.

Overview

Federal law requires the NOC to provide situational awareness and a common operating picture for the entire federal Government, and for state, local, and tribal governments as appropriate, and to ensure that critical disaster-related information reaches government decision makers. *See* Section 515 of the Homeland Security Act (6 U.S.C. § 321d(b)(1)). The law defines the term "situational awareness" as "information gathered from a variety of sources that, when communicated to emergency managers and decision makers, can form the basis for incident management decision-making." OPS is launching this Initiative to fulfill its legal mandate to provide situational awareness and establish a common operating picture directly related to the security, safety, and emergency response associated with the BP oil spill off the Gulf Coast.

The NOC is using Internet-based platforms that provide a variety of ways to follow activity related to the BP oil spill response by monitoring publicly available online forums, blogs, public websites, and message boards. Through the use of publicly available search engines and content aggregators[1] the NOC continuously monitors activities on social media sites, such as those listed in Appendix A, for information directly relevant to the BP oil spill response so the NOC can provide situational awareness and establish a common operating picture. The NOC gathers, stores, analyzes, and disseminates relevant and appropriate de-identified information to federal, state, local, and foreign governments, and private sector partners authorized to receive situational awareness and a common operating picture.

The NOC is identifying and monitoring only information directly related to the security, safety, and emergency response associated with the BP oil spill in Louisiana. The NOC will use this information to fulfill the statutory mandate set forth above to include the sharing of information with foreign governments and the private sector as otherwise authorized by law. The NOC will not:

[1] Content aggregators generally provide a consolidated view of web content in a single browser display or desktop application.

- Seek, collect, or retain any PII or other information in an identifiable form;
- Conduct any social networking where the Department's employees are required to establish a username and password to gain access to information; and
- Seek to establish individual identities or connect with other individuals' identities.

Should PII come into the NOC's possession, the NOC shall redact it prior to further dissemination of any collected information.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

The NOC is reviewing information posted by individual account users on third party social media providers of activities and events necessary to provide situational awareness and establish a common operating picture regarding the security, safety, and emergency response associated with the BP oil spill response off the Gulf Coast. Third party service providers provide an array of applications that provide social media services along with publicly available online forums, blogs, public websites, and message boards. See Appendix A for a list of the types of sites that may be viewed for information related to the BP oil spill response. The NOC is accessing these web-based platforms to identify content posted by public users for the purpose of providing situational awareness and establishing a common operating picture on the BP oil spill response. The NOC is assessing information identified to assist decision-makers in the security, safety, and emergency response associated with the BP oil spill. The NOC shall not collect data on the individuals posting information to third party service providers, about individual users, or any PII. The NOC will immediately destroy any PII that it discovers at any time in its possession as a result of this Initiative.

1.2 What are the sources of the information in the system?

Members of the public as well as first responders, press, volunteers, and others provide publicly available information on social medial sites including online forums, blogs, public websites, and message boards.

1.3 Why is the information being collected, used, disseminated, or maintained?

The NOC is identifying, using, disseminating, and maintaining this information to comply with its statutory mandate to provide situational awareness and establish a common operating picture for the entire federal government, and for state, local, and tribal governments as appropriate and to ensure that this information reaches government decision makers. In this case, the NOC is monitoring information directly related to the security, safety, and emergency response associated with the BP oil spill off the Gulf Coast. The aggregation of data published via social media sites will likely make it possible for the NOC to provide more accurate situational awareness, a more complete common operating picture, and more timely BP oil

spill response-related information for decision makers.

1.4 How is the information collected?

The NOC identifies information directly from third-party social media services. The NOC is accessing and collecting information from various informational streams and postings that the NOC, as well as the broader public, view and monitor.

1.5 How will the information be checked for accuracy?

The NOC identifies information from third party hosts submitted voluntarily by members of the public and compares that information with information available in open source reporting and through a variety of public and government sources. By bringing together and comparing many different sources of information, the NOC will attempt to generate a more accurate picture of activities occurring at the BP oil spill site off the Gulf Coast.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

Congress requires the NOC "to provide situational awareness and establish a common operating picture for the entire federal government and for state, local, and tribal governments as appropriate, in the event of a natural disaster, act of terrorism, or other manmade disaster; and ensure that critical terrorism and disaster-related information reaches government decision-makers." Section 515 of the Homeland Security Act (6 U.S.C. § 321d(b)(1)). The BP oil spill is a manmade disaster.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

There is a risk that the NOC will receive PII or other identifiable information that is not relevant to this Initiative. The NOC has a clear policy in place that any PII incidentally received will be redacted immediately. Information collected to provide situational awareness and establish a common operating picture originates from publicly available social media sites and is available to the public.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The NOC is using Internet-based platforms that provide a variety of ways to follow activities related to the BP oil spill response off the Gulf Coast, by monitoring publicly available online forums, blogs, public websites, and message boards. Through the use of publicly available search engines and content aggregators, the NOC will continuously monitor activities on social media sites, such as those listed in Appendix A, for information directly relevant to the BP oil spill response. The NOC will gather, store, analyze, and disseminate relevant and appropriate information to federal, state, local, and foreign governments, and private sector partners requiring and authorized to receive situational awareness and a common operating picture.

2.2 What types of tools are used to analyze data and what type of data may be produced?

NOC analysts are responsible for monitoring and evaluating information provided on social media sites. The overall analysis will be used to provide situational awareness and establish a common operating picture.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

Publicly available, user-generated data can be useful to decision-makers as it provides "on-the-ground" information to help corroborate information received through official sources.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

As the NOC does not collect or use any PII, the risk to privacy is that PII will be brought into the NOC unintentionally. This has been mitigated by the clear policy that any PII inadvertently collected shall be redacted immediately.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

The NOC will retain only user-generated information posted to publicly available online social media sites. Information posted in the public sphere that the Department uses to provide situational awareness or establish a common operating picture or sent to the Department in connection with the BP oil spill response becomes a federal record and the Department is required to maintain a copy. However, the Department is working with the National Archives and Records Administration (NARA) on a retention schedule to immediately delete PII, upon the approval of this schedule by NARA.

3.2 How long is information retained?

The NOC will retain information only long enough to provide situational awareness and establish a common operating picture. The Department is working with NARA on a retention schedule to immediately delete PII, upon the approval of this schedule by NARA.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

The Office of Records Management is working with NARA to establish an approved retention and disposal policy.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

The risk associated with retention of information is that PII will be retained when it is not necessary and that the information will be kept longer than is necessary. The NOC has mitigated this risk by redacting PII it inadvertently collects and is working with NARA on a retention schedule to immediately delete PII, upon the approval of this schedule by NARA.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Information related to the BP oil spill response is shared within the NOC, with Departmental leadership, and with those components within the Department involved in the security, safety, and emergency response associated with the BP oil spill. The NOC is sharing this information for the statutorily mandated purpose of providing situational awareness and establishing a common operating picture.

4.2 How is the information transmitted or disclosed?

Information is transmitted via email and telephone within the NOC and to the Department's components where necessary and appropriate. PII is not collected, but if pushed to the NOC, it will be redacted by the NOC before information is shared. The remaining data is analyzed and prepared for reporting.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

The risk associated with sharing this information is that PII will be inadvertently collected and shared. The NOC has mitigated this risk by establishing effective policies to avoid collection of PII and to redact it if collected inadvertently. Additionally, the NOC will not conduct any social networking where individuals are required to establish a user name and password to gain access to information. Instead, the NOC is only monitoring publicly accessible sites where users post information voluntarily.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

The NOC is using this Initiative to fulfill its statutory responsibility to provide situational awareness and establish a common operating picture for the entire federal government, and for state, local, and tribal governments as appropriate, and to ensure that critical disaster-related information reaches government decision makers. Information may also be shared with private sector and international partners where necessary, appropriate, and authorized by law.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

PII is not actively collected. Information is only collected to provide situational awareness and to establish a common operating picture.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Information is shared by phone, email, and other paper and electronic form.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

External sharing risks are minimal as the Initiative does not share PII; only information collected to provide situational awareness and to establish a common operating picture is shared.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

The Department may publicize its use of social media. The NOC does not, however, provide notice to specific public users who voluntarily provide user-generated information on publicly accessible social media sites where individuals are not required to establish a user name and password to gain access to information. The NOC may retrieve public information from the social media sites, but will not respond to individual users as no accounts will be created.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Information posted to social media websites is publicly accessible and voluntarily generated. Thus, the opportunity not to provide information exists prior to the informational post by the user.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Individuals voluntarily post information on social media sites and have the ability to restrict access to their posts as they see fit. Any information posted publicly can be used by the NOC in providing situational awareness and establishing a common operating picture.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

There is no requirement to provide notice to individuals under the framework applied under this Initiative. Information posted to social media approved for monitoring under this Initiative is publicly accessible without a password and voluntarily generated. There is no reasonable expectation of privacy for such information.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

Social media are public websites. All users have access to their information through their user accounts. Individuals should consult the privacy policies of the services they subscribe to for more information.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Users may accidentally or purposefully generate inaccurate or erroneous information. There is no mechanism for correcting this. However, the community is largely self-governing and erroneous information is normally expunged or debated rather quickly by others within the community with more accurate and/or truthful information.

7.3 How are individuals notified of the procedures for correcting their information?

There is no specified procedure for correcting information; if there was, it relates to a social media provided process and not a DHS process. Individuals may change their PII on the sites as well as the accessibility of their content posts at any time they wish through their user account management tools on social media sites.

7.4 If no formal redress is provided, what alternatives are available to the individual?

There is no specified procedure for correcting information; if there was, it relates to a social media-provided process and not a DHS process. Individuals may change their PII as well as the accessibility of their content posts at any time they wish through their user account management tools on the social media sites. Individuals should consult the privacy policies of the services to which they subscribe for more information.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

The information available on social networking websites is largely user-generated, which means that the individual chooses the amount of information available about himself/herself as well as the ease with which it can be accessed by other users. Thus, the primary account holder should be able to redress any concerns through the third party host of the service. Individuals should consult the privacy policies of the services they subscribe to for more information.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

No procedures are in place. Social media sites are publicly available, third-party services.

8.2 Will Department contractors have access to the system?

Yes, as it is required in the performance of their contractual duties at DHS.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All DHS employees and contractors are required to take annual privacy training.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

No.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

This PIA is effective for 60 days and will expire at that time. Should the requirements for the Initiative change before this expiration date, OPS and the Privacy Office will immediately update this PIA.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

These social media sites are publicly available, third-party services. Information is collected by the service itself to establish an account. Thereafter, users determine their level of involvement and decide how "visible" they wish their presence on any given service to be. The ability to choose how much information to disclose, as well as the short period of retention for any information collected by the NOC serves to mitigate any privacy risk.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

Third parties control and operate these services. Users should consult with representatives of the service provider in order to make themselves aware of technologies utilized by the system.

9.2 What stage of development is the system in and what project development lifecycle was used?

Social media is active at all times and is third-party owned and operated.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

Individuals should consult the privacy policies of the services they subscribe to for more information.

Responsible Officials

Donald Triner
Director (Acting), National Operations Center
Office of Operations Coordination and Planning
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office.

_____

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

APPENDIX A

Examples of Social Media Web Sites Monitored by the NOC

This list is not comprehensive, but provides a list of the types of sites that the NOC is reviewing in order to improve its situational awareness and establish a common operating picture related to the BP oil spill response in Louisiana.

Collecta	http://collecta.com
RSSOwl	http://www.rssowl.org/
Social Mention	http://socialmention.com/
Spy	http://www.spy.appspot.com
Who's Talkin	http://www.whostalkin.com/
Hulu	http://www.hulu.com
iReport.com	http://www.ireport.com/
Live Leak	http://www.liveleak.com/
Magma	http://mag.ma/
Time Tube	http://www.dipity.com/mashups/timetube
Vimeo	http://www.vimeo.com
Youtube	http://www.youtube.com
MySpace Video	http://vids.myspace.com/
Global Incident Map	http://globalincidentmap.com/
IBISEYE	http://www.ibiseye.com/
Stormpulse	http://www.stormpulse.com/
Trends Map	http://www.trendsmap.com
Flickr	http://www.flickr.com/
Picfog	http://picfog.com/
Twicsy	http://www.twicsy.com
Twitcaps	http://www.twitcaps.com
Monitter	http://www.monitter.com/
Twazzup	http://www.twazzup.com
Tweefind	http://www.tweefind.com/
Tweetgrid	http://tweetgrid.com/
Tweetzi	http://tweetzi.com/
Twitter Search	http://search.twitter.com/advanced

ABCNews Blotter	http://abcnews.go.com/Blotter/
Accuweather	http://www.accuweather.com/
BNOnews	http://www.bnonews.com/
British Petroleum	http://www.bp.com/bodycopyarticle.do?categoryId=1&contentId=7052055
Coast Guard Social Media Hub	http://uscg.mil/socialmedia/
Crisisblogger	http://crisisblogger.wordpress.com/
Danger Room	http://www.wired.com/dangerroom/
DownstreamToday	http://www.downstreamtoday.com
Drudge Report	http://drudgereport.com/
Emergency Management Magazine	http://www.emergencymgmt.com
Environmental News Network	http://www.enn.com/
Foreign Policy Passport	http://blog.foreignpolicy.com/
Google Blog Search	http://blogsearch.google.com
Gulf of Mexico - Transocean Drilling Incident	http://www.piersystem.com/go/site/2931/
Homeland Security Today	http://www.hstoday.us/
Homeland Security Watch	http://www.hlswatch.com/
Huffington Post	http://huffingtonpost.com/
InciWeb	http://www.inciweb.org/
iReport	http://www.ireport.com/
LA Now	http://latimesblogs.latimes.com/lanow/
National Geographic	http://www.nationalgeographic.com/
National Defense Magazine	http://www.nationaldefensemagazine.org
National Terror Alert	http://www.nationalterroralert.com/
NASA Earth Observatory	http://earthobservatory.nasa.gov/
Newsweek Blogs	http://blog.newsweek.com/
NOLA	http://www.nola.com/
NYTimes Lede Blog	http://thelede.blogs.nytimes.com/
Popular Science Blogs	http://www.popsci.com/
Port Strategy	http://www.portstrategy.com/
Public Intelligence	http://publicintelligence.net/
ReliefWeb	http://www.reliefweb.int
RigZone	http://www.rigzone.com/
Science Daily	http://www.sciencedaily.com/
Technorati	http://technorati.com/
The Latin Americanist	http://ourlatinamerica.blogspot.com/
The Weather Channel	http://www.weather.com/
United Nations IRIN	http://www.irinnews.org/
Upstream Online	http://www.upstreamonline.com/
USA Today On Deadline	http://content.usatoday.com/communities/ondeadline/index/
Weather Underground	http://www.wunderground.com/
WireUpdate	http://wireupdate.com/