

## One Step Ahead: How Social Media is Changing the Face of Investigations

One third of investigators still do not have the resources to utilize social media properly for investigations.

## Table of Contents

Industry Insights Overview.....	3
The 21st Century Criminal .....	3
The 21st Century Investigation .....	4
One Step Ahead – Anticipation And Prediction.....	5
Social Media And Legal Compliance.....	6
Social Media Starts At The Top .....	7
Conclusion .....	7

## Industry Insights Overview

The methods criminals leverage in an attempt to plan, organize and perpetrate crimes are evolving rapidly – shifting from a “street corner” approach to establishing and using social networks. This digital interaction is challenging law enforcement officers to keep pace, many of them turning to social media to aid in investigations. In fact, in the *LexisNexis® 2012 Law Enforcement Personnel Use of Social Media in Investigations Study* of over 1,200 federal, state and local active duty officers indicated that four out of five respondents use various social media platforms to assist in investigations. Social media has also made inroads into the courtroom, where search warrants utilizing social media information to establish probable cause hold up in court in nearly nine out of ten instances.

Unfortunately, despite social media’s proven track record in law enforcement, only half of those in command positions support its use during investigations and critical incidents. Without support from advocates at the top, adequate legal & tactical training, proper access and investigative tools, social media becomes a risky choice for analysts and detectives should their case go to trial. This industry insight provides compelling information about why social media intelligence gathering using a robust data mining tool should be part of every agency’s policing strategy – encouraged from the top down – to solve crime and to help predict criminal behavior.

## The 21st Century Criminal

The world has gone social. Society has moved towards a platform of self-promotion and sharing personal information with the masses. People now turn to Twitter to communicate upcoming plans with friends. Facebook is replacing personal email communication. People use social media to discuss the mundane, but to also promote political and social options. Those who use social media often forget that their digital footprints last forever, saved in the massive databases used by the platforms.

Criminals are utilizing social media, the same way many of us are, but also for covert illegal activities. They are becoming more sophisticated in their approach to crime, utilizing Twitter, Facebook, Instagram and YouTube, whenever possible. Social media is the new medium they are using to organize, advertise and publicize their illicit activities. Street corner solicitation for drugs and prostitution are now conducted in social media, and if your detectives and analysts aren’t online everyday tracking this activity, you are missing critical intelligence on criminal activity in your community.

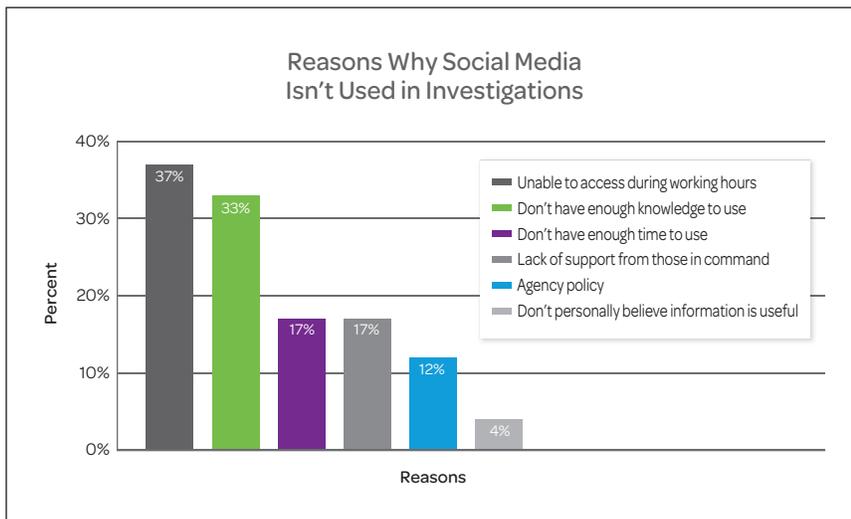
During the 2011 Stanley Cup playoffs, the Vancouver Police Department investigated riots, which were organized and fueled through social media, resulting in several arrests based on videos, photos and comments posted on Facebook and Twitter. Without open access to social media, covert profiles and knowledge of how the platforms were being used, investigators may not have been able to respond and act as quickly to the riots. Consequently, if investigators had tools to monitor social media sites, they may have been able to disrupt these riots before they occurred or escalated.

If your detectives are not aware of how social media has changed the way people communicate and how criminals conduct illicit activities, they are missing critical evidence and investigative leads.

As society has integrated social media into the fabric of their lives, people expect law enforcement to adapt and integrate social media into their daily operations. Many law enforcement agencies throughout the country have embraced the need to communicate and engage with their constituents via social media. Unfortunately, law enforcement is still slow to embrace social media as an indispensable tool in the investigative tool box.

## The 21st Century Investigation

Spending hours burning shoe leather by going door to door to follow up on leads is becoming a thing of the past. Detectives who are only using traditional investigative practices to canvass and to follow up on tips are missing huge investigative opportunities and leads by not consulting social media sites.



Although there are some agencies that see the value of monitoring social media information, they may not be using their personnel's time efficiently. Monitoring social sites for potential criminal activity is time consuming and tedious. Putting a detective on desk duty to troll hundreds of social media sites each day is a waste of a valuable resources and often nets little intelligence on impending criminal activity.

If your detectives are not aware of how social media has changed the way people communicate, they are missing critical evidence and leads. During the critical hours after a violent crime, detectives must canvass the area for witnesses, gather statements, corroborate information, sift through evidence and run down every viable lead. Multiple investigators, support personnel and analysts are often needed to take on all of these tasks in order to quickly solve the case. With shrinking budgets, often times due diligence suffers because of other, more pressing cases, staffing issues and a lack of resources. These resource issues can lead to missed witnesses and stalls in the investigation. Tools like LexisNexis@Social Media Monitor help alleviate many of these personnel-focused tasks by using data harvesting, key words and automated searches to locate social media activity before, during and after a crime.

In the *LexisNexis® 2012 Law Enforcement Personnel Use of Social Media in Investigations Study*, law enforcement officers showed that 37% did not utilize social media during investigations because of a lack of access to these sites (firewalls on department-issued computers) and 17% did not have time to use these sites. Time and access issues can be solved with a multifunctional social media monitoring solution that automates searches, making access easy and the information gathered timely.

Social Media Monitor, a new function of Accurint® for Law Enforcement, allows agencies to discover risks and diffuse threats using social media. This new capability can alert officers to potential areas of concern and help them identify posts or tweets within specific geographic locations. This adds a virtual dimension to investigations enabling law enforcement to verify identities, uncover non-obvious associations and generate a comprehensive view of a suspect.

In today's digital world, canvassing is not only going from house to house and knocking on doors, but it is taking a digital snapshot of social media activity in the immediate area where a crime occurred. Using sites like Twitter, Google+, Instagram and Facebook, it is impossible to find every possible piece of social media data that was generated before, during and after a crime occurred. It would also take an investigator or analyst countless hours and he or she would miss critical data. But with a tool like Social Media Monitor providing continuous, proactive automated monitoring of almost all social media sites so that investigators and analysts are not tied to their desks. It also provides the ability for detectives to quickly access near real time data from social media sites like Twitter, Instagram, Facebook and YouTube, keeping them up to date with what is going on in near real-time in a certain area.

By using social media data, along with other traditional law enforcement data, investigators can determine if criminal behavior is likely to be repeated. Integrating public records and traditional law enforcement data with social media data provides a complete picture of what crime could be committed.

## One Step Ahead – Anticipation and Prediction

Investigating crimes that have already been committed is one piece of the social media puzzle; providing predictive capabilities about criminal events is the next step. Integrating social media data into the intelligence analysis function will help with crime anticipation, crime prediction and crime disruption. With social media, investigators can gather intelligence to understand where suspects have been, with whom they have associated and what they have done in the past. Using this data, along with other traditional law enforcement data, investigators can determine if criminal behavior is likely to be repeated. Integrating public records and traditional law enforcement data with social media data provides a complete picture of what crime *could be* committed. Social Media Monitor provides the ability to set search terms and alerts on keywords and phrases that are found in incident and intelligence reports, offering valuable insights to help officers disrupt and stop potential crimes and criminal activity.

Instead of manual searching and monitoring, automated alerts of words used to describe drugs, gang activity or firearms could be used to free up personnel for other, more proactive investigative work. These types of automated alerts can be easily added to Social Media Monitor so that investigators and analysts are only alerted when that word or phrase appears in a new social media post, in a specific geographic area. These alerts help analysts develop intelligence on locations and targets before an incident happens.

Picking up on “chatter” through automated alerts also provides enhanced officer safety for those in sensitive or undercover assignments. For example, Social Media Monitor assisted gang investigators with keeping one of their own safe when there was a gang-related shooting in a major metropolitan area. A gang member posted information through his social media account about an undercover officer, who was posing as a gang member. Police officers, who were monitoring the social media activity of that individual, were able to see the “chatter” about this undercover officer and realized that the officer was in danger and needed to be removed from the assignment immediately. The ability to see this real-time social dialogue saved the officer’s life and provided key evidence and intelligence into the prior shooting. It also gave investigators the ability to archive that social media data, as it appeared at the time of the threat, so that it could be used later for prosecution as key evidence.

The crime anticipation, prediction and disruption capabilities offered by social media can best be summed up by one example from a law enforcement officer – responding to the 2012 PoliceOne survey – who shared how social media provided information on a “terroristic threat involving students in a local high school. Further investigation (using Facebook) revealed the threats were credible and we conducted follow-up investigations which revealed a student intent on harming others. The student was in the process of attempting to acquire weapons. It’s my belief we avoided a ‘Columbine’ type scenario.”

Command level support of social media use in investigations and for intelligence gathering is critical. This support must be in the form of training, policies and robust tools that make accessing and mining social media sites quick and easy.

## Social Media and Legal Compliance

Policies concerning the use of social media for intelligence gathering and investigations, as well as training on legal updates, is critical to compliance. Policies must be consistent with laws, regulations and other agency-specific policies and must be updated regularly to reflect any new legal rulings. If your agency is using social media for investigations without these policies and legal training in place, your cases may be in jeopardy and your agency could come under political fire. The International Association of Chiefs of Police (IACP) Center for Social Media was created to help Chiefs and Sheriffs create policies, provide officers training and understand the most recent trends in how social media is being used to support investigations and major incidents. The IACP’s website [www.theiacp.org](http://www.theiacp.org) provides resources for agencies starting out with social media and for those integrating social media into the fabric of their policing strategy.

It is imperative that agencies are compliant with how they use information obtained via social media sites within their investigative process. Without clear guidelines, your agency is open to potential violations of 28 CFR Part 23. Tools like Social Media Monitor provide an archive function to preserve information gathered that is legally compliant and admissible in court. Social Media Monitor keeps an agency compliant with laws related to intelligence gathering and ensures that departments will be able to admit this evidence in court.

## Social Media Starts at the Top

Command level support of social media use in investigations and for intelligence gathering is critical. This support must be in the form of open access to social media sites, training on legal updates, policies on use for investigations and robust tools that make accessing and mining social media sites quick and easy. Without this type of support, investigators and analysts are left to spin their wheels, possibly make errors that may have legal repercussions and waste countless hours trying to learn the ins and outs of social media sites. Even more important is arming detectives and analysts with legally compliant monitoring and analytical tools, like Social Media Monitor, to help them uncover information about suspects, crimes and evidence.

Chiefs and Sheriffs should invest in tools like Social Media Monitor as another way to develop and verify intelligence. This tool will save already strapped departments time and money and will protect them from legal issues that could arise from using social media incorrectly. Social Media Monitor is as critical a tool as a Computer Aided Dispatch (CAD) system, a mapping software or a case management system. Without this critical tool to automate searches and archive the information found, hundreds of personnel hours will be lost to manual online searches, door knocks and running down false leads. Key online data will be lost without an archiving function that preserves the text and images as they were posted for future admissibility in court. Your detectives and analysts need this type of tool to stay one step ahead of criminals in your community.

## Conclusion

Criminals have gone digital. It is absolutely crucial for law enforcement agencies to implement a comprehensive social media investigative strategy that includes data mining tools, to address this emerging criminal landscape. The strategy should span all levels – federal, state and local – it should incorporate dedicated, trained personnel, and employ tools like Social Media Monitor. Adoption needs to start at the top through command-level support, which includes clear policy, investment in sophisticated analytical software, as well as the training of staff to effectively create actionable intelligence from this data. Investigators and analysts need social media data not only to look for suspects after a crime is committed, but to gather actionable intelligence to stay one step ahead.

Social media mining tools, like Social Media Monitor, will give detectives and analysts significant time back to focus on other crimes and investigations. It streamlines social media sites into one easy to use tool, alerts users to new activity and archives posts for future reference and usage. It also provides command staff with information to stop criminal activity before it occurs. Ultimately, the use of social media for investigations will increase operational efficiencies and address budget restrictions, representing a tremendous opportunity for today's front-line officers to keep our streets safe.

Social media is a new technology and 70% of law enforcement officers who have used it are essentially self-taught. Any social media solution should be easy to use, fitting neatly into an officer's existing workflow.

**For more information:**

**Call 888.579.7638 or visit  
[lexisnexis.com/risk](http://lexisnexis.com/risk)**

**About LexisNexis® Risk Solutions**

LexisNexis Risk Solutions ([www.lexisnexis.com/risk](http://www.lexisnexis.com/risk)) is a leader in providing essential information that helps customers across all industries and government predict, assess and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, we provide products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of Reed Elsevier, a leading publisher and information provider that serves customers in more than 100 countries with more than 30,000 employees worldwide.



LexisNexis, the Knowledge Burst logo and Martindale-Hubbell are registered trademarks of Reed Elsevier Properties Inc., used under license. Bridger Insight is a trademark of LexisNexis Risk Solutions Inc. Other products or services may be trademarks or registered trademarks of their respective companies. This document is for educational purposes only and does not guarantee the functionality or features of LexisNexis products identified. LexisNexis does not warrant this document is complete or error-free. If written by a third party, the opinions may not represent the opinions of LexisNexis. The LexisNexis® Social Media Monitor services are not provided by "consumer reporting agencies," as that term is defined in the Fair Credit Reporting Act (15 U.S.C. §1681, et seq.) ("FCRA") and do not constitute "consumer reports," as that term is defined in the FCRA. Accordingly, the LexisNexis® Social Media Monitor service may not be used in whole or in part as a factor in determining eligibility for credit, insurance, employment or another purpose in connection with which a consumer report may be used under the FCRA. Other products or services referenced may be trademarks or registered trademarks of their respective companies. © 2013 LexisNexis. All rights reserved. NXR05040-0 1013