Social Media Policy and Law Enforcement Investigations

Todd G. Shipley, CFE, CFCE
President & CEO
Vere Software

VERE SOFTWARE
INVESTIGATIVE TOOLS

Agenda

- Social Media is changing how some law enforcement agencies approach criminal investigations.

- A properly written social media investigations policy should guide managers and investigators use of social media during investigations.

How SM is being adopted by Users

Law Enforcement

The Rest of the World

“I’m from the Government and I am here to help…”

Break the law and your new 'friend' may be the FBI

By RICHARD LARDNER (AP) – Mar 16, 2010

WASHINGTON — The Feds are on Facebook. And MySpace, LinkedIn and Twitter, too.

U.S. law enforcement agents are following the rest of the Internet world into popular social-networking services, going undercover with false online profiles to communicate with suspects and gather private information, according to an internal Justice Department document that offers a tantalizing glimpse of issues related to privacy and crime-fighting.

Think you know who's behind that "friend" request? Think again. Your new "friend" just might be the FBI.

The document, obtained in a Freedom of Information Act lawsuit, makes clear that U.S. agents are already logging on surreptitiously to exchange messages with suspects, identify a target's friends or relatives and browse private information such as postings, personal photographs and video clips.

AP Associated Press

Photo 1 of 2

FILE - In this Oct. 13, 2009, file photo, Assistant U.S. Attorney Michael Scoville displays part of the Facebook page, and an enlarged profile photo, of fugitive Maxi Sopo in Seattle. The Feds are on Facebook. And

VERE SOFTWARE INVESTIGATIVE TOOLS

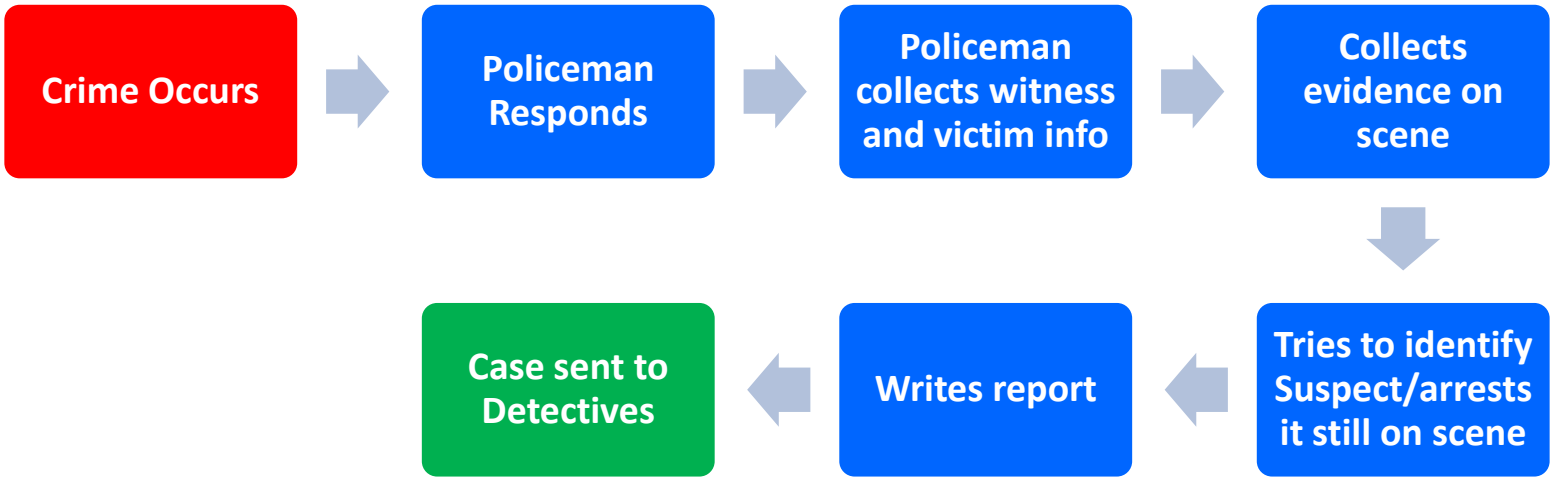
Fear of LE use of Social Networking

Why We Use Social Media in Our Investigations?

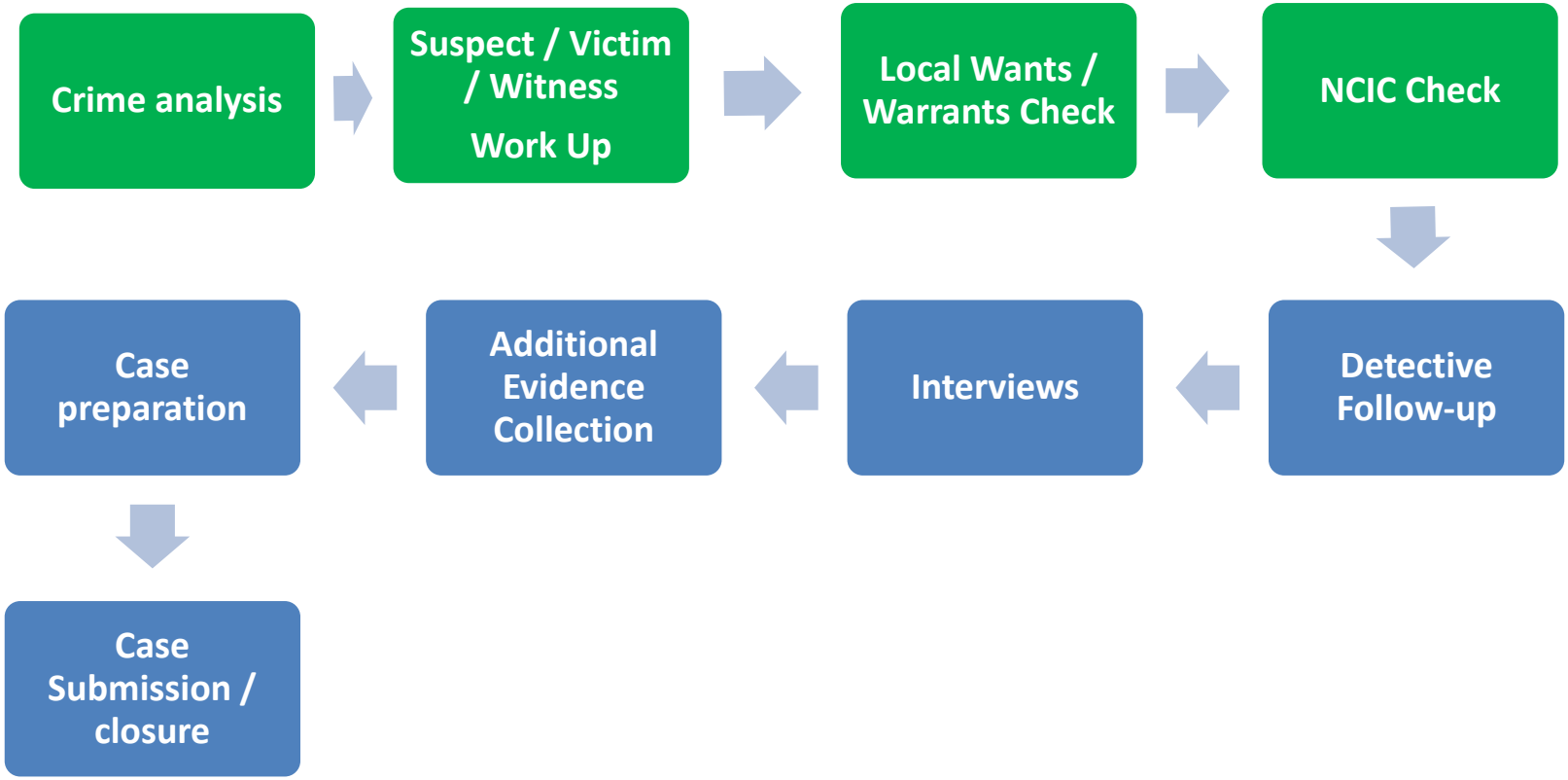
- ✓Locate evidence of crimes
- ✓Obtain criminal Intelligence
- ✓Gain useful background on suspects/victims
- ✓Lead Generation

Each of these usually has some department policy directing this kind of investigation.

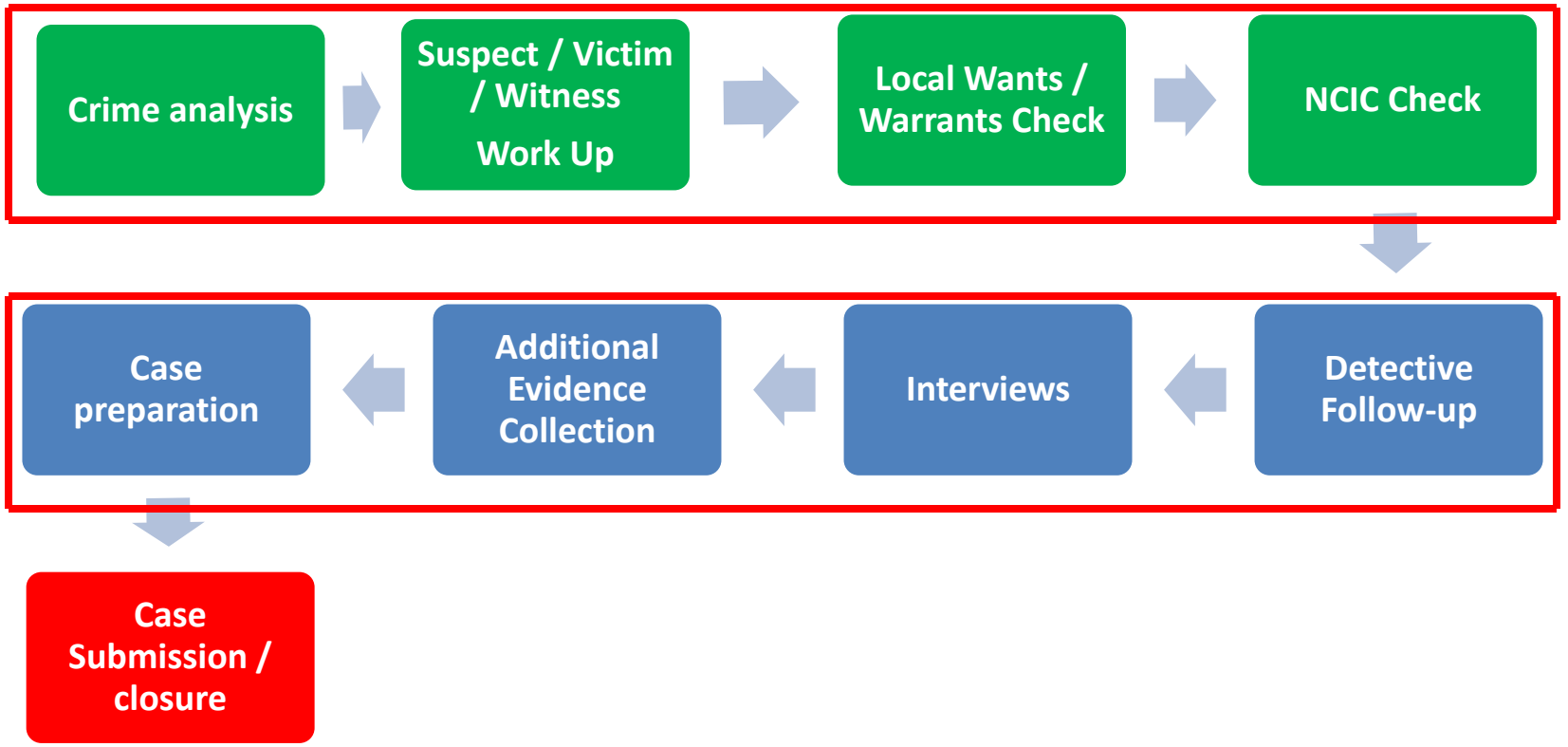
General LE Investigation Response



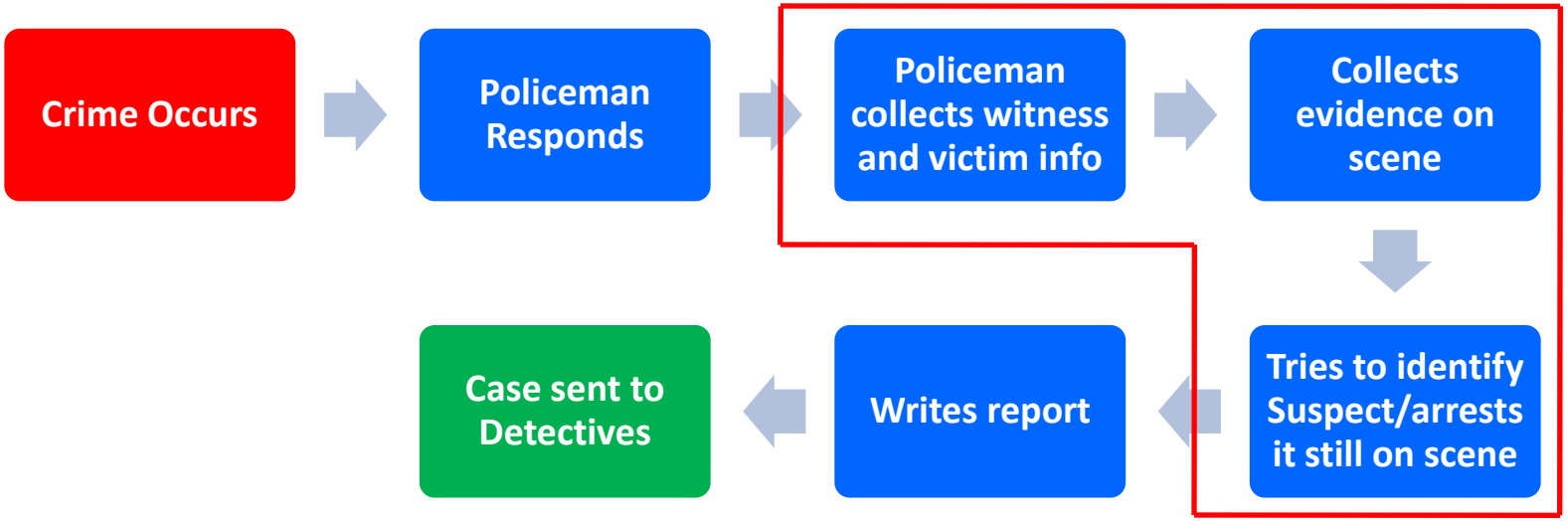
Investigative Response



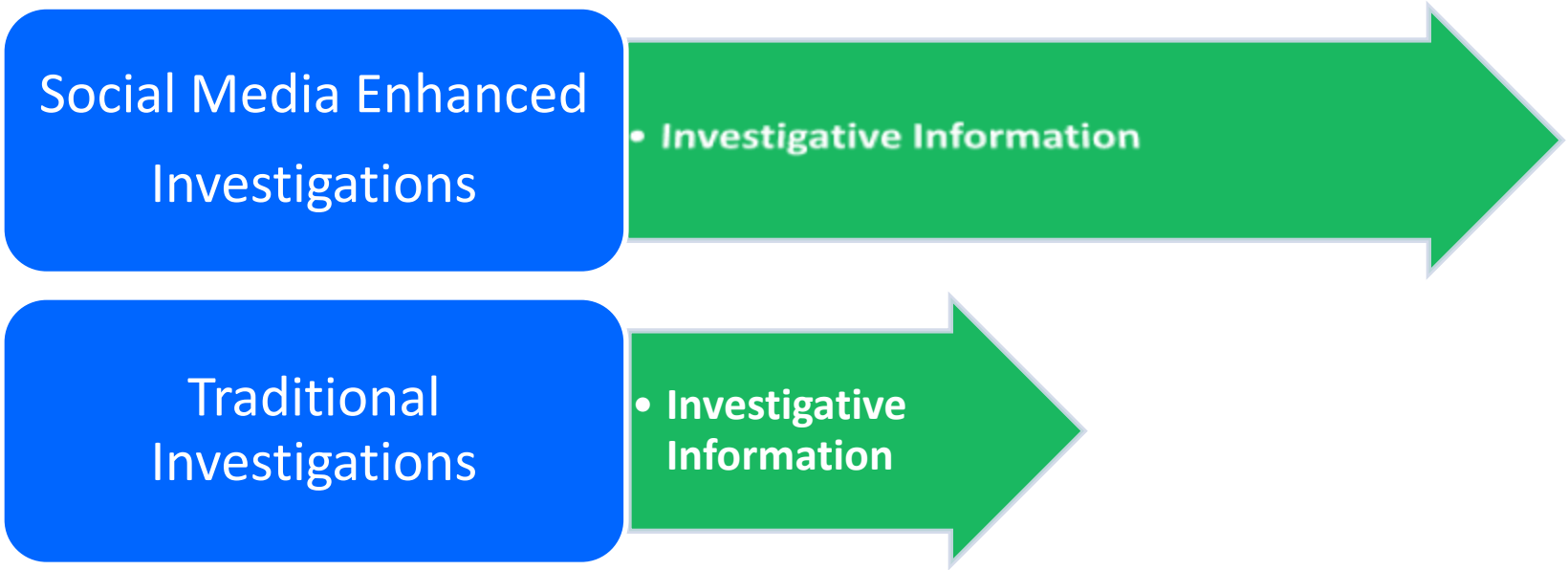
Where Does SM Fit Into your Investigations?



General LE Investigation Response



SM vs. Traditional Investigations

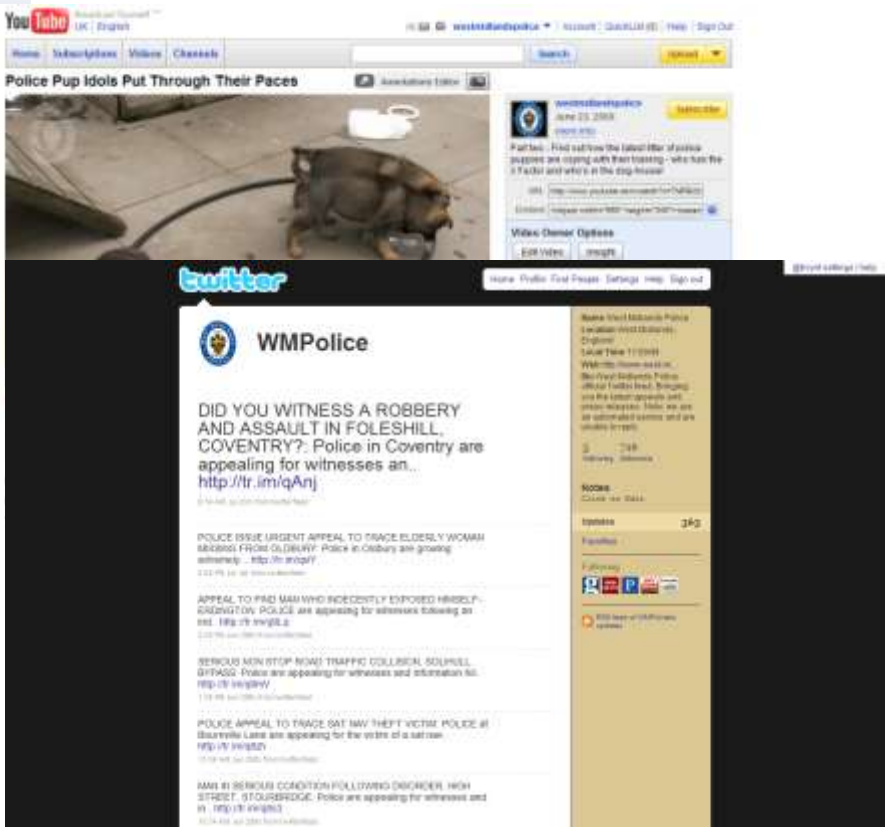


When SM Could Be Used

- Large Scale Law Enforcement responses

Alberto Martinez/Austin-American Statesman, via Associated Press

When LE is Effectively Using SM



VERE SOFTWARE
INVESTIGATIVE TOOLS

Why a SM Investigation Policy

- Traditional Investigations
  - Supervisor assigns case
  - Monitors reports
  - Dictates case requirements
- Online Investigations
  - Supervisor assigns case
  - Monitors reports
  - Dictates case requirements
- Traditional UC Investigations
  - Supervisor on scene
  - Listening to wire
  - Watching operations
- UC Investigations Online
  - Supervisor isn't sitting over investigators shoulder watching hours of online chat.
  - Generally reviews content post the investigators actions.

Why a SM Investigation Policy

- Traditional Investigations
  - Supervisor assigns case
  - Monitors reports
  - Dictates case requirements

- Traditional UC Investigations
  - Supervisor on scene
  - Listening to wire
  - Watching operations

POLICY

- Online Investigations
  - Supervisor assigns case
  - Monitors reports
  - Dictates case requirements

- UC Investigations Online
  - Supervisor isn't sitting over investigators shoulder watching hours of online chat.
  - Generally reviews content post the investigators actions.

Why a SM Investigation Policy

- Traditional Investigations
  - Supervisor assigns case
  - Monitors reports
  - Dictates case requirements

- Traditional UC Investigations
  - Supervisor on scene
  - Listening to wire
  - Watching operations

NO POLICY

- Online Investigations
  - Supervisor assigns case
  - Monitors reports
  - Dictates case requirements

- UC Investigations Online
  - Supervisor isn't sitting over investigators shoulder watching hours of online chat.
  - Generally reviews content post the investigators actions.

➢ ***Policy should clearly lay out guidance for supervision of and conduct of investigations.***

Designing your SM Investigation Policy

- Social Networking investigations have no different requirements when it comes to documenting the investigations.

- The investigative techniques applied on the Internet still require the information be properly collected, properly preserved and properly presented in a report.

Professional Conduct Online

- Officers realize their obligation to the community and should strive to act in a professional manner while investigating crimes on the Internet in order to inspire the public trust and confidence.
- Maintaining professionalism, even while online, should be a primary goal our officers and will ensure the continued trust and respect of the community.
- All officers are public servants and shall keep all contacts with the public both professional and courteous.

Deciding to Conduct Proactive SM Investigations Online

- Requires agency policy decisions
- Evaluation of internal capabilities
- External Opportunities (Task Forces)
- Cost evaluation (equipment and personnel)

Policy for Conducting SM Proactive Ops

- Covert undercover operations on the Internet and Social Networking are an effective investigative technique.
- The ultimate goal of any online undercover operation is a criminal conviction.
- Every aspect of undercover operations should be well planned, deliberate and performed in compliance with all applicable policies.
- The actions of undercover officers on the Internet should always be appropriate, under the circumstances, and easily justified to prosecutors, judges and juries.

Policy for Conducting SM Proactive Ops

- Obtain supervisory approval.
- Corroborate undercover investigations with other officers conducting surveillance , use of informants and cooperating suspect(s).
- Only utilize investigative computer systems and software intended to record data from the internet and audio and/or video recording in an evidentiary manner when contacting suspects.

Policy for Conducting SM Proactive Ops

- Officers will not transfer or make available for download any files that they knowingly contain any malicious code or other type of file that would disrupt, delay, or destroy another person's computer system,
- Officers will follow all local guidelines and Federal law when conducing undercover operation on social networking sites.

Proactive Online Investigations

- Online proactive strategies can be as controversial as real world operations if you do not consider the issue of entrapment.
- Many courts cases have dealt with this issue
  - The basic rule is: A police officer can provide the opportunity, or can encourage the offender to act, but he cannot compel the behavior.
- A fine line to tread.

Proactive Social Networking Investigations

- UC operations will only be used when such use is proportionate to the seriousness of the offence(s) being investigated (and the history and character of the individual(s) concerned).
- Online UC operations should not be used as a speculative means of search for the existence of a criminal offense, where no other grounds exist to suspect that criminal offenses have been or are being committed

Online Proactive Operational Plans

- Operational plans for the conduct of proactive operations on social networking are intended to guide officers through the execution of an enforcement action.

- They provide for the assignment of personnel, identification of suspects, equipment and locations (both physical and online) and play a significant role in the safety of officers involved.

Deconfliction

- Potential for multiple agencies to be conducting similar investigations on the same criminal suspects, website, social networking sites or organizations at any given time.
- Safety considerations in such situations that may bring law enforcement investigators into high-risk situations without realizing the presence of other law enforcement Investigators.
- Parallel investigations, conducted independently, are less efficient and effective than cooperative law enforcement efforts conducted in a coordinated manner.

Terms of Service

- Social networking sites require that users, when they sign up, agree to abide by a terms of service (TOS) document.

  - Agency employees are responsible for reading and understanding the TOS of the sites they use during an undercover investigation.
  - TOS agreements may ban users who give false names or other false information during the registration process which may affect the investigation if the use of an undercover identity is discovered by the social networking site

Other Policy Considerations for Online Operations

- Participation in Otherwise illegal Activity by Undercover Employees
- Review of Conduct
- Protecting Innocent Parties Against Entrapment
- Identifying and Managing Employee Stress

Documenting Online Investigations

- All data recorded and video or audio recordings made from the social networking site being used in the investigation shall be considered as evidence and handled as such, regardless of the quality of the recording.

- All video and audio recordings will be maintained as evidence until the case receives a final disposition.

Social Networking Use Model Policy

- Model Policy For Agency use of SN
- Model Policy For LE Investigative use of SN
- Model Policy For Off-Duty LE use of SN

*Will be available from Vere Software website at www.veresoftware.com

"Make the Internet your regular beat."

Internet Evidence: Collection | Preservation | Presentation

VERE SOFTWARE
INVESTIGATIVE TOOLS

Serving and Protecting the World Wide Web

4790 Caughlin Pkwy, #323
Reno, Nevada 89519
USA

Toll Free: 888.432.4445
E-mail: info@veresoftware.com
Web: www.veresoftware.com

VERE SOFTWARE
INVESTIGATIVE TOOLS