PRIORITY
Criminal Justice
NEEDS INITIATIVE
A project of the RAND Corporation, the Police Executive Research Forum, RTI International, and the University of Denver

Using Social Media and Social Network Analysis in Law Enforcement

Creating a Research Agenda, Including Business Cases, Protections, and Technology Needs

John S. Hollywood, Michael J. D. Vermeer, Dulani Woods, Sean E. Goodison, Brian A. Jackson

In April 2017, the National Institute of Justice convened an expert panel to assess, and identify high-priority needs for, law enforcement's use of two closely linked technologies that have potential to provide key information needed to address crime risks, hold offenders accountable, and ensure physical safety: social media analysis and social network analysis. Social media analysis consists of methods and tools to collect and analyze text, photos, video, and other material shared via social media systems, such as Facebook and Twitter. Social network analysis is a type of data analysis that investigates social relationships and structures as represented by networks (which can also be called graphs). Social media, given that it reflects relationships inherently, is a key source of data for social network analysis; conversely, social network analysis is one key type of social media analysis.

In all, the panel discussed five core business cases for employing social media analysis and social network analysis in law enforcement:

1. **Social media analysis:** Monitoring for activity indicating short-term safety threats in postings, and communicating responses as needed.
2. **Social network analysis, possibly with social media data:** Identifying those at high risk for involvement in violence.
3. **Social media analysis:** Actively monitoring the high-risk to see whether violence may be imminent.
4. **Social media analysis and social network analysis:** Investigating organized crime networks.
5. **Social media analysis and social network analysis:** Investigating crimes.

The panel also discussed one core case not to do:

1. Monitoring First Amendment–protected activity for vague or unspecified purposes.

Key Findings

- Expert panelists characterized business cases for employing social media and social network analysis in law enforcement, including monitoring for short-term safety threats in postings; identifying those at high risk of involvement in violence, either acutely or chronically; and investigating specific crimes and organized crime networks.
- The panel also specified a core case not to do: monitoring of First Amendment–protected activity for vague purposes.
- The panel specified a framework for providing computer security, privacy, and civil rights protections when employing social media and social network analysis.
- Finally, the panel identified and prioritized needs for innovation related to social media and social network analysis. The four themes of this innovation agenda are (1) supporting working with communities to develop policies and strategies for using social media analysis and social network analysis; (2) technical development, starting with assessing current tools and how they might be better tailored to law enforcement; (3) law enforcement–specific training on these types of analysis; and (4) creation of a help desk to help law enforcement agencies navigate requests to social media companies and interpret the resulting data.

The panel identified a framework for providing computer security and protecting privacy and civil rights. This framework is shown in Figure S.1 and consists of the following types of protections:

- **Data protections** ensure that legal backing is there for all data collected for law enforcement purposes; that covert and undercover operations using social media analysis similarly have legal backing; and that the collected information is protected from both external and insider threats.
- **Analysis protections** similarly ensure that legal backing is there for all law enforcement analyses, and that analysis results are protected from external and insider threats. More broadly, these protections help ensure equitable justice outcomes by protecting against inaccuracies and biases.
- **Action protections** ensure that policing practices are not distorted and that both enforcement and social service actions are employed consistently and equitably.

The core business cases and protection framework elements are outlined in this report.

Reflecting both the business cases and the protection framework, the expert panel identified a series of needs for innovation to better support the use of social media and social network analysis in law enforcement. These needs fall across four themes that define an innovation agenda (Figure S.2) to support the appropriate and sustainable use of these tools for public safety purposes.

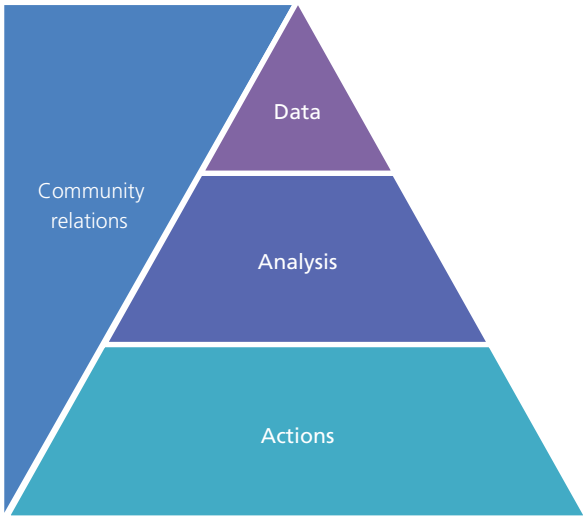
The first part of our expert panel's innovation agenda is to support working with communities to develop policies and strategies for using social media and social network analysis. Here, the initial recommendations relate to developing and disseminating best practices for transparency and collaborative decisionmaking for employing social media and social network analysis technologies, as well as collaboratively creating a series of model policies for employing and securing these types of analysis.

The second part of the agenda is technical research on law enforcement–specific social media and social network analysis. The initial recommendation is to assess the capabilities of current tools and methods and how they might be better tailored to law enforcement, with the first step of that assessment being to create and disseminate a market survey of what tools and methods are found useful by practitioners now and how well they are working.

The third part of the agenda is supporting law enforcement–specific training on social media and social network analysis. Here, the initial recommendations are to develop requirements for training and assess gaps between current commercial- and defense-focused training and what is needed for law enforcement training. This implicitly includes studies and analyses of what tools and methods are working best in support of law enforcement operations. Training on legal implications and protections is a short-term need that can be addressed by developing a model curriculum.

The final part of the panel's innovation agenda is a help desk to help law enforcement agencies navigate requests to social media companies. The help desk would help agencies with making process requests more likely to result in data returns and/or content takedowns that address the needs of specific cases; it would also help agencies process and interpret the data returned from process requests.

Figure S.1. An Initial Privacy, Security, and Civil Rights Protection Framework



RAND *RR2301-S.1*

Figure S.2. The Innovation Agenda

RAND *RR2301-S.2*

INTRODUCTION

Many modern communication and analytic technologies are becoming mature enough that they are increasingly accessible to the average law enforcement organization. Responsible access and analysis of these technologies hold promise for identifying and halting crime threats, investigating crimes and holding offenders responsible, and detecting and responding effectively to emergencies and hazards (all of which are core objectives of law enforcement; see Hollywood et al., 2015, pp. 4–6). At the same time, law enforcement access to and analyses of communications data raise concerns about, and require protections for, individual privacy, civil rights, and information security.

This report describes an expert panel's deliberations on two such key and closely interlinked communications technologies: *social media analysis* and *social network analysis*. The panel brought together both practitioners and researchers with experience in using these technologies within law enforcement applications. Figure 1 summarizes these two technologies and their relationships.

Social media analysis consists of methods and tools to collect and analyze text, photos, video, and other material shared via social media systems, such as Facebook, Twitter, YouTube, Instagram, Pinterest, and Snapchat. Social network analysis is one type of analysis used in analyzing social media data. Social media is important today, as a communication and interaction mode for people in general and as both a "venue" and an enabler for certain types of crime. Law enforcement interaction with social media and use of social media data is therefore important, given the need to police in this technological era. However, social media analysis by law enforcement does raise acute privacy, security, and civil rights needs, because of the ubiquitous nature of the technology and because social media is commonly used for sensitive and private discussions.

Social network analysis is a type of data analysis that investigates social structures as represented by networks (which can also be called *graphs*). In these networks, each person is a "node" or "vertex," and each relationship between pairs of people is a link (also called an "edge" or "tie"). Figure 2 shows an example social network diagram.

Social media, given that it reflects relationships inherently, is a key source of data for social network analysis; conversely, social network analysis is one key type of social media analysis.

Often, the purpose of social network analysis is to identify the most "important" or "central" node in a network; how "important" or "central" is defined varies but is usually based on the number and types of relationships a person has. As examples:

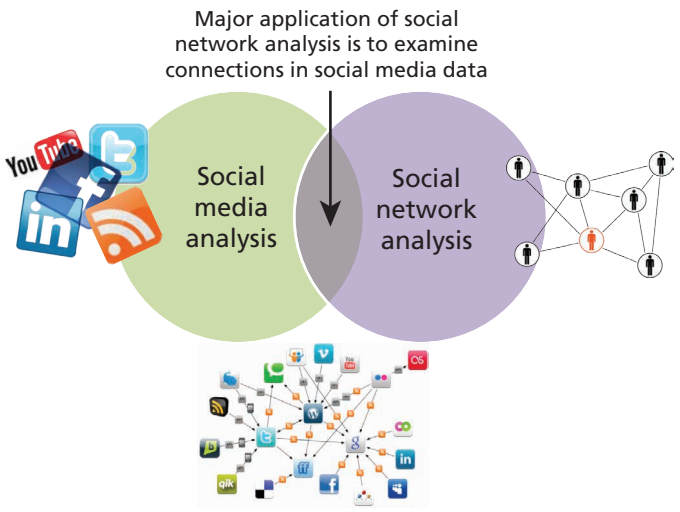
- A person who has more links (i.e., known direct relationships) than others has a high "degree centrality."
- A person who acts in a bridging role, linking different subgroups that would otherwise not be related to each other, has a high "betweenness centrality."
- A person who has a high number of indirect relationships, meaning that the person is related to others who in turn have a high number of direct links, also tends to have leadership and influence.

Also of interest is the ability to recognize subgroups or subcommunities within a larger social network; a law enforcement example would be to help break a criminal social network down into likely gangs and cliques within gangs. As an example, one recent paper identified methods to recognize gangs and likely members of gangs within a larger social network (Paulo et al., 2013).

Figure 3 adds examples of nodes with high degree centrality and high betweenness centrality, as well as subgroups, to the network shown in Figure 2.

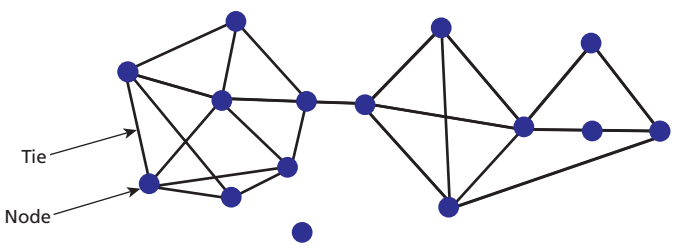
When conducting analyses like this, a node is typically a person, but it does not have to be. Social network analysis can

Figure 1. Social Media and Social Network Analysis



RAND *RR2301-1*

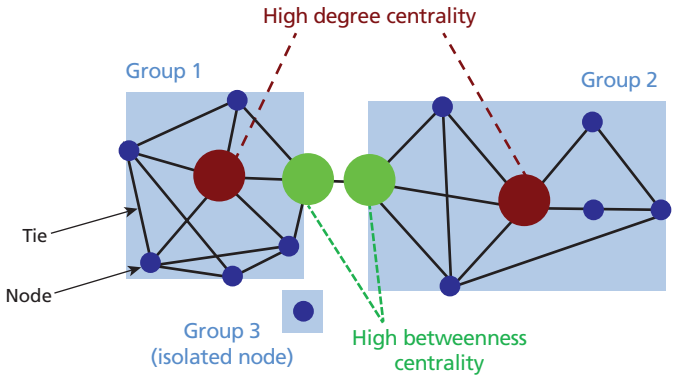
Figure 2. Example Social Network Diagram (Sociogram)



SOURCE: Coldren and Markovic, 2015, p. 14.

RAND *RR2301-3*

Figure 3. Central Nodes and Network Subgroups



RAND *RR2301-3*

also be used to identify important links to assets (vehicles, financial accounts) and addresses.

Scott (2012) and Hannemann and Riddle (2005) provide example textbooks that are useful in educating analysts on how to make use of social network analysis. Ahajjam, El Haddad, and Badir (2018) provide an example of a contemporary method for identifying likely influencers and leaders in social networks (in brief, these influencers/leaders typically have higher numbers of both direct and indirect relationships). Girvan and Newman (2002) provide an example of a method for finding likely subgroups within larger social networks.

Given that social media data are inherently networked, providing information about people and their relationships as symbolized through communications, analysis of social media data often relies on social network analysis. The Social Media Research Foundation's NodeXL is an example of a social network analysis tool that includes capabilities to import data from social media platforms, including Facebook, Twitter, YouTube, and Flickr (2016). Pew Research Center (2014) provides an example of conducting social network analysis on Twitter networks. That said, social network analysis can use any law enforcement data that provide information on entities (people, locations, addresses, etc.) and their relationships. Examples include record management system (RMS) enforcement and incident data, field reports and interview data, tips from the public, and call-for-service data.

As the use of social media platforms has become almost ubiquitous in modern society, including among offenders and organized crime networks, social media is becoming a key source of information about both threatened and actual criminal activity. There have been multiple high-profile cases where, after a violent act has already been perpetrated, investigators found what appear to have been indicators or "warning signs" that might have been detected and followed up on to prevent the event. The field of social network analysis studies the relationships between people and assets and can, among other things, identify those with "central" roles in criminal networks; social network analysis naturally provides methods for analyzing social media data for investigative purposes.

Recent cases, law enforcement presentations, and published accounts provide a range of examples of the use of social media data and social network analysis for law enforcement purposes:

- Solving a gang-related shooting by matching knowledge about feuding gang networks with motor vehicle information. Analysts used social network information to identify potential adversaries of a victim with gang connections. They then queried to see which gang associate owned the vehicle that matched a witness's description (Cheung and Prox, 2012).
- Watching posts and videos uploaded to YouTube made by a particular gang, in which gang members described their criminal activities and made explicit threats against others. This use does require being able to distinguish between genuine criminal evidence and "false positive" postings and relationships (e.g., Popper, 2014). More broadly, police have used evidence of crimes posted online, including offenders posting photos of crime scenes and bragging about them, to hold offenders accountable (Dughi, 2016).
- Prioritizing subjects for gang call-ins and enhanced enforcement and prosecution based on how central they were in criminal gang networks (Coldren and Markovic, 2015).

Social media is growing in importance to law enforcement. LexisNexis has reported that, as of a 2014 survey of law enforcement professionals who use social media operationally at least to some extent, 86 percent used social media for investigations two to three times per month, and 25 percent reported using it daily (LexisNexis Risk Solutions, 2014). At the same time, there have been substantial concerns about the usage of these tools. In the same survey, only 48 percent of respondents said that their agencies had formal processes on social media investigations, and only 9 percent reported receiving training from their agency.

With respect to social network analysis, the mapping of networks has been a part of law enforcement investigation for many years, and new tools provide increased capability. Using tools that generate networking diagrams (also known as "link charts") is common, and the creation of networking diagrams is a core feature in tools such as Coplink Analyst's Notebook and Palantir Technologies' products. However, the spread of more-advanced algorithms that leverage cutting-edge academic research in social network analysis is more limited, and those techniques are much less known in law enforcement (e.g., Coldren and Markovic, 2015).

METHODOLOGY

To assess the expanding importance of social media and social network analysis in law enforcement, we assembled an expert panel to (1) consider applications and protections for employing social media and social network analysis and (2) then identify and prioritize needs for innovation related to use of these types of analysis and associated analytics in law enforcement. Panel members included a range of experts, including practitioners of social media and social network analysis in law enforcement, developers of social media and social network analysis methods for law enforcement, and researchers and attorneys with expertise on community advocacy, privacy, and civil rights issues related to these types of analysis. Panelists were identified through a collection of literature reviews (including both scientific articles and recent conference and workshop presentations) and assistance from National Institute of Justice and Bureau of Justice Assistance staff.

We engaged the panel to achieve two purposes. The first, given the relative newness of using these types of analysis in law enforcement, was to provide insight to the law enforcement community, including practitioners, funders, and developers, on how these technologies might be used and secured effectively. This included

- identifying emerging applications for using social media data and social network analysis in law enforcement, and capturing key process steps and considerations in business cases
- identifying a core set of security, privacy, and civil rights protections when using social media data and social network analysis in law enforcement.

Given that law enforcement use of social media and social network analysis is still relatively new and is controversial for a variety of reasons, the intent was to contribute to and advance policy debate on these issues. The effort was intended to survey both the promise and challenges of these technologies, and to frame areas where additional research and attention were warranted, *not* to provide definitive guidance or propose model policy for their use.

The second purpose was to identify specific needs for innovation to help law enforcement make better use of social media data and social network analysis. We define a need as a requirement put forward by the panel for research, development, or dissemination of a product or service to help solve a problem or take advantage of an opportunity. "Products" can include nonmaterial items such as new policies, regulations, processes, analytic techniques, and organizational structures, in addition to physical systems.

Appendix A, the Technical Supplement, provides the technical details of the generation and prioritization of the needs. In summary, to frame the panel discussion, prior to the workshop, we sent out a read-ahead and had participants fill out an online questionnaire. The questionnaire asked panelists to identify specific operational questions that social media data

Workshop Participants

Jeff Asher
Journalist; formerly with New Orleans Police Department

Charles L. Cohen
Indiana State Police

Dawn Diedrich
Georgia Bureau of Investigation

Andrew Ferguson
University of the District of Columbia

Kevin Hiner
City of Richmond, Va., Police Department

Rachel Levinson-Waldman
Brennan Center

John Markovic
Bureau of Justice Assistance

Michael G. Mastronardy
Ocean County, N.J., Sheriff's Office

Joe McHale
Marion, Iowa, Police Department

Patrick Muscat
Wayne County, Michigan, Prosecutor's Office

Desmond Patton
Columbia University School of Social Work

Jay Stanley
American Civil Liberties Union

Wendy H. Stiver
Dayton, Ohio, Police Department

Lee Tien
Electronic Frontier Foundation

Michael Yu
Montgomery County, Md., Department of Police

and social network analysis tools should answer; which questions social media data and social network analysis tools should not help answer; what specific security, privacy, and civil rights protections are needed; and specific problems or opportunities related to social media data and social network analysis that should be discussed at the workshop. In addition to providing a way for panelists to contribute to shaping the discussion during the meeting, the questionnaire also helped to define a common framework for identifying top issues and developing needs for innovation to address those issues.

Developing business cases for applications of social media and social network analysis. A business case is a description of a potential project or task that provides enough clarity on what is to be done to support making resource allocation decisions about it (e.g., Herman and Siegelaub, 2009). Given the relative novelty of these types of analysis to law enforcement, this project included working with the panel to identify major applications of social media and social network analysis for law enforcement and develop business cases for them. Our descriptions include

- describing what the applications are and what law enforcement objectives they support
- describing the core steps in the business process to carry out the applications, including providing process flow diagrams
- describing both known recommended and inadvisable actions needed to carry out the applications successfully and avoid political and legal pitfalls.

The business cases can be thought of as a simplified and generalized version of technical use cases. We do not use "use case" terminology here, as use cases commonly involve detailed technical documentation, including Unified Modeling Language (UML) use case diagrams that were not an intended product of our effort (for example, Adolph, Cockburn, and Bramble, 2002).

Most of the panel's discussion of business cases focused on the operational questions that social media and social network analysis tools should or should not help answer, as well as protections that were needed. As business cases were developed at the workshop, we asked panelists to add specific steps that were needed, specific technologies that were needed, and tips on should-dos and should-not-dos. Following the workshop, the notes from these discussions were grouped and edited into major business cases for social media and social network analysis.

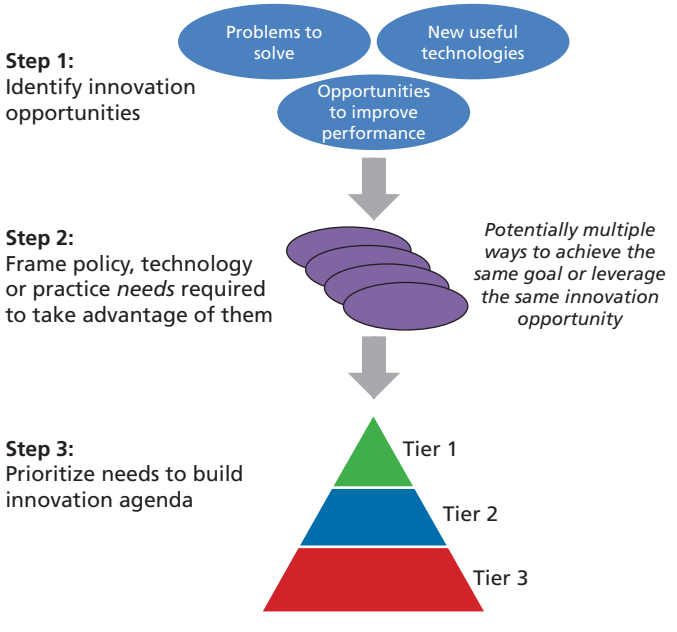
Needs-generating and needs-prioritizing process. After the business case discussion, the panel turned to discussing and prioritizing needs. The process is summarized in Figure 4.

The first step is to identify "innovation opportunities": problems to address, or opportunities to take advantage of, to better support law enforcement objectives and core business cases. The panel began with the set of problems and opportunities from the questionnaire, and added to it during the workshop. The second step was to propose one or more solutions for each problem or opportunity—a specific idea for an *innovation*, which can be technical but can also concern policy, practice, organization, or training. In our work, each need consists of a problem/opportunity statement and a solution statement. There can be multiple solution statements—and hence multiple needs—for the same problem/opportunity, capturing different options or strategies that are available.

To make it possible to identify needs that were more important to pursue, in the third step, we asked the panel to prioritize the needs that came out of the discussion. To do so, the panelists scored each need for two measures: potential importance if the need was successfully met, and likelihood that it could be successfully met (in general). Each measure was rated on a scale of 1 to 9, with 1 being low and 9 being high, using an online questionnaire.

Using a similar methodology as prior Priority Criminal Justice Needs Initiative studies, we then generated median expected value scores and divided the needs into three tiers by

Figure 4. Identifying and Prioritizing Needs for Innovation



RAND *RR2301-4*

their median score (as shown in Figure 4), using a hierarchical clustering algorithm. Our focus is on the cluster of needs with the highest scores, Tier 1. (Tier 2 constituted the cluster with middle-scoring needs, while Tier 3 constituted the cluster with the lowest-scoring needs.) That said, we also capture needs with very high importance scores, even if they had high risk scores (and thus were not in Tier 1). *Priority needs* met at least one of the following criteria:

- Tier 1 (top expected value tier out of three tiers), as identified from the hierarchical clustering algorithm
- Tier 2 but with a high median importance to law enforcement (median potential importance at 8 or higher). These can be thought of as high-risk, high-reward needs.
- Tier 2 but with the same or greater median ratings for individual measures as other Tier 1 needs. This group included one need that had an identical proposed solution to another Tier 1 need; it just addressed a different problem statement.

We then grouped the priority needs into common themes, and used the priority needs and themes to develop an *innovation agenda* (proposed way ahead) for social media and social network analysis for law enforcement.

Appendix A presents the full methodology and results of using the clustering algorithm to prioritize needs along with additional analyses to identify high-risk, high-reward needs.

Identifying overarching themes. To identify top themes reflecting groups of needs, we first created a network (or graph) of needs by defining links between pairs of needs if the needs addressed similar issues or proposed the same type of solution. Displaying the network revealed that the needs and their relationships fell into four entirely separate groups. The similarities between the four separate groups gave rise to the four major themes identified by the expert panel (see below).

BUSINESS CASES FOR SOCIAL MEDIA AND SOCIAL NETWORK ANALYSIS

Table 1 shows the business cases developed by the group, along with whether they pertain to social media analysis, social network analysis (including data besides social media postings), or both, based on the panel's discussions. These business cases are discussed further below.

Monitoring Social Media for Worrisome Activity

> We saw posts to organize a massive protest. Then we saw the scary part—the organizers asking for advice, as none of them had ever organized an event before. We swung into action and helped them with all the things you need to do to have a safe event.
>
> —comment during the workshop

This business case concerns using social media feeds to provide alerts to law enforcement. In general, the panel discussed that this application is for *safety purposes*—detecting emergencies, potential crimes or terror attacks in progress, event security, and so on—rather than criminal justice investigative purposes. Figure 5 shows the business process diagram for this business case.

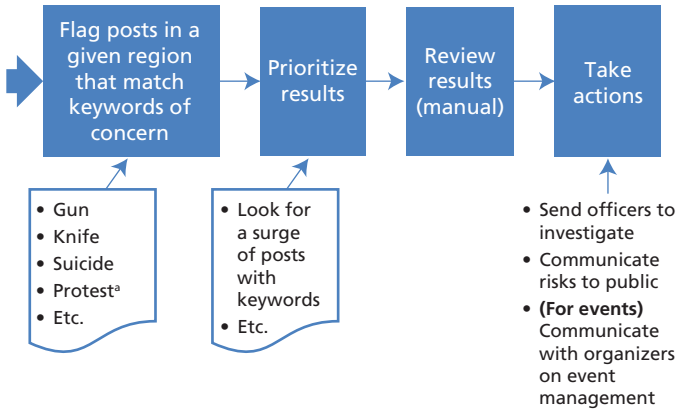
The panel spent a great deal of time discussing what sorts of situations warranted monitoring, and a rough consensus emerged. First, pervasive, wide-ranging monitoring of the general public's First Amendment–protected speech on social media for uncertain purposes was not seen as appropriate, as it constitutes an invasion of privacy and could imply governmental surveillance (and potential suppression) of lawful speech.

Conversely, the panelists concurred that monitoring a crowded event (sports events, festivals, theme parks) for narrowly described posts implying crimes or emergencies in progress was considered appropriate. Panelists discussed success

Table 1. Business Cases for Social Media and Social Network Analysis

Business Case	Relevant to Social Media Analysis?	Relevant to Social Network Analysis?
Monitoring for worrisome activity	√	
Identifying those at high risk for involvement in violence		√
Actively monitoring high-risk situations	√	√
Investigating organized crime networks	√	√
Investigating specific crimes	√	√

Figure 5. Monitoring Social Media for Worrisome Activity



[a] Problematic—mitigated if for safety/event management purposes.

RAND *RR2301-5*

stories here in rapidly detecting (nonlethal) bomb explosions and suicide attempts. Similarly, panelists noted that monitoring a specific suspect's posts as part of a criminal investigation was appropriate. Note that such monitoring is not technically part of this business case—it is covered in other business cases.

As for cases between the extremes above, the discussion focused on how these needed to be worked out at the local level, community by community. This led to panel discussions on the need for transparency and how to engage communities more effectively, with the Privacy Advisory Council of Oakland, California, used as an example (City of Oakland, 2017).

The group noted that some of the social media monitoring applications that have attracted the most concern have had to do with law enforcement agencies monitoring First Amendment–protected speech for reasons appearing to fall outside of public safety or policing. Some panelists suggested that these problematic applications may be from commercial technology providers attempting to adapt existing monitoring applications designed for commercial, advertising, or other non–public safety purposes to law enforcement to broaden the market for existing (or modestly modified) tools. For example, a commercial sales pitch along the lines of

> Wouldn't you like to know who uses your product, what they think about it, and where they are? Now you can!

might be naïvely converted for a law enforcement audience, without regard to concerns about monitoring of First Amendment–protected speech:

> Wouldn't you like to know who the #TodaysProtestGroup's supporters are, what they think, and where they are? Now you can!

Panelists also noted false positive issues in monitoring social media. Keyword searches have frequently returned irrelevant posts, giving law enforcement staff too many postings to wade through to identify real emergencies.

An emerging trend within this business case is integrating social media into calls for service. Panelists discussed a future in which social media text posts, images, and video could all be part of emergency "calls" that would get into public safety access points (PSAPs). Next Generation 911 is in part intended to address this need (National Telecommunications and Information Administration, 2017). Agencies would then have the capability to retransmit information to officers who need it over emerging LTE and wireless networks (this was discussed in detail at the National Institute of Justice's workshop on future broadband communications technologies; see Hollywood et al., 2016). However, there are many issues to address, starting with how to verify incoming data and validate the information's time and location. Panelists described a case in which a reported image of a man pointing a gun at a toddler was ultimately found to have come from overseas and was likely a hoax.

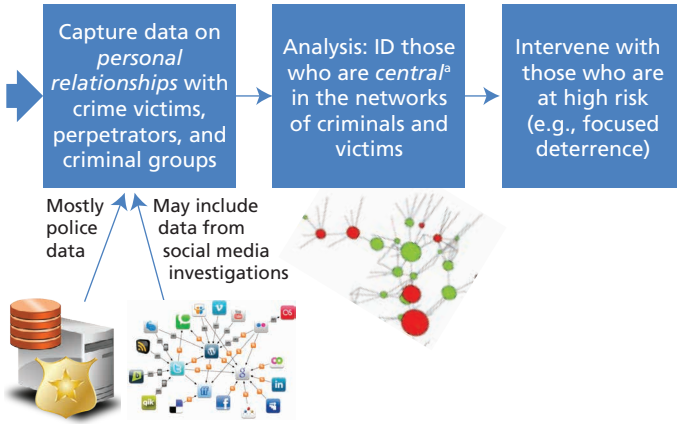
Identifying Those at High Risk for Involvement in Violence

This business case relates to identifying and intervening with persons who are at high risk of being involved in violence (and, potentially, other major crimes as well), whether as a perpetrator, victim, or both. Here, increased risk of being engaged in or targeted for violence is determined through a combination of social media postings and other law enforcement tips. Risk is also determined through relationships to others involved in violence and other major crimes (as detected through co-arrest records, field interview reports, social media connections, and other relationship data), as well as additional quantitative data about a person. Figure 6 shows the business process diagram for this case.

Interpreting social media and other law enforcement data is discussed in more detail in the next business case. This case focuses more on using social network analysis and analysis of other quantitative data to identify those most at risk of involvement in violence. Here, social media data are seen primarily as an input, used to identify and characterize social relationships.

As noted, high-risk individuals tend to be *central* in the social networks of those involved in crime (e.g., Green, Horel, and Papachristos, 2017; Papachristos, Wildeman, and Roberto, 2015). Here, being central typically relates to "degree

Figure 6. Identifying Persons at High Risk for Involvement in Violence



[a] The definition of central varies by method used.

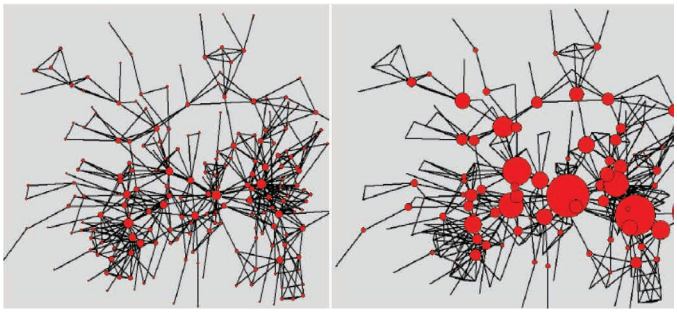
RAND *RR2301-6*

centrality"—having comparatively large numbers of links to others involved in criminal activity, either directly or indirectly (for subjects who link to others who, in turn, are linked to many others). It also relates to people with high "betweenness centrality"—that is, those who are intersections on many paths of links between others in the network. In Figure 7, the left image highlights those with a high number of relationship links to others (degree centrality), while the right image highlights those who are on many paths of connections within the network (betweenness centrality).

Ways to get to social network analysis and other quantitative data include the following:

- Manually done assessments of specific criminal gangs of interest, typically focusing on those gangs believed to be the most violent in a jurisdictional area. Analysts might start with "gang audits," combining interviews with field officers, information provided by community members, and law enforcement intelligence sources to identify persons and relationships within criminal gang networks, including both same-gang links, affiliated gang links, and adversarial or conflict links. Coldren and Markovic (2015)'s training session describes the use of gang audits in Chicago and Kansas City, Missouri (see also Fox et al., 2014).
- Reviewing field reports, incident reports, and other law enforcement data to capture relationship links.
- Reviewing social media postings and videos to capture relationships, such as people appearing in the same photos and videos, and threats made against specified persons in groups.
- Counting co-arrest links with others who went on to become homicide victims or nonlethal gunshot victims.

Figure 7. Degree- and Betweenness-Central Persons in Social Networks



SOURCE: Coldren and Markovic, 2015, pp. 24–25.

RAND *RR2301-7*

A co-arrest link refers to a case in which one person is arrested with another person who goes on to become a victim of violence. Research has shown that subjects who have numbers of co-arrest links that make them part of social networks with members suffering lots of violent attacks are likely to be parties of violence themselves (Green, Horel, and Papachristos, 2017; Papachristos, Wildeman, and Roberto, 2015).

For whatever type of data is used, accuracy and timeliness of data are key to making correct assessments. Understanding the local context of the information is also important; see the "Monitoring High-Risk Situations" business case below.

The principal type of intervention done with those at risk for being a party to violence is focused deterrence (also known as "pulling levers"), which combines the promise of enhanced punishments for engaging in violence with incentives for desisting from violence (or high-risk behavior, more generally). The interventions also include meetings in which subjects are told of the negative consequences of engaging in violence, including the impact that engaging in violence is having on their families and communities, and the positive consequences of desisting from violence. Incentives typically include increased assistance in accessing a range of social services; sanctions typically include increased contacts with law enforcement, increased investigations and prosecutions, and increased sentencing on conviction.

The National Network for Safe Communities (2016) provides a general guide to an exemplar focused deterrence intervention, the Group Violence Intervention. Braga, Weisburd, and Turchan (2018) provide a review and evaluation of focused deterrence interventions, finding the class of interventions to be promising in reducing violence. In general, the panel noted that highly punitive interventions raise far more privacy and civil rights concerns than do providing services. Panelists noted that

with proactive risk-reduction measures such as focused deterrence, care must be taken to avoid punishing people for crimes they might commit in the future but have not actually committed. Similarly, analysts need to be able to differentiate between people who are high-risk because they are a high threat to the community versus those who are at high risk of becoming a victim (chronic substance users, chronic gamblers, low-level street dealers, those who are related to high-threat persons, etc.), and tailor interventions accordingly.

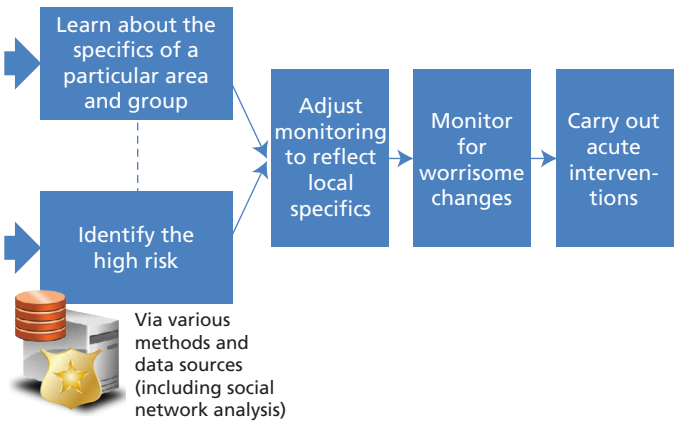
Monitoring High-Risk Situations

This case concerns monitoring specific high-risk situations—feuding criminal gangs within or across neighborhood borders, for example—and detecting and intervening on information implying that acts of violence could be imminent, starting with warning potential victims. This case is about detecting and acting on immediate, near-term, acute threats, whereas the prior case is about detecting and acting on chronic threats. The two cases can interact with each other: People at higher risk of involvement with violence can be monitored during high-risk situations, while people who become parties to high-risk situations can be referred to focused deterrence interventions.

Figure 8 shows a business process diagram for this case. In the figure, it is presumed that social network analysis helps identify which persons, groups, and relationships are most pressing to monitor, while social media analytics help detect worrisome events and changes regarding those persons, groups, and relationships.

This application requires actively engaging with a specific community to understand the underlying situations. Analysts must understand local contexts—otherwise, they will not be able to tell benign communications from genuinely threatening communications, even before any concealment efforts by individuals seeking to obscure the meaning of their postings are considered. One cannot just look for "threatening" keywords or images; panelists noted cases in which posting music lyrics or pictures of guns for general deterrence purposes were falsely considered to be threats. Panelists suggested that one strategy could be involving local youths in efforts to "translate" postings and language to help identify genuine threats.

Figure 8. Active Monitoring of High-Risk Situations



RAND *RR2301-8*

Investigating Organized Crime and Specific Crimes

These were mentioned at the workshop, but the panel did not develop detailed use cases for them at the conference, perhaps because the application of these analytical techniques is more established in traditional organized crime investigation.

For social network analysis, the panel noted that viewing networks of criminal associates could provide a great deal of situational awareness and aid in investigating crimes. A network surrounding a crime victim or other crime-related entities (addresses, vehicles, etc.) provides immediate lists of persons and other entities of interest. As examples, a 2013 FBI bulletin presented applications of identifying why two rival gangs suddenly started battling each other; identifying a previously unknown associate of an at-large suspect, which put pressure on that suspect to surrender; and piecing together a network of convenience store robberies and the persons responsible (Johnson et al. [2013] and Bichler and Malm [2015] provide additional examples).

For social media analysis, the panelists discussed observed criminal activity and evidence for investigations of specific crimes in postings, tweets, videos, photos, and other social media feeds and posts. Most of the panel's time on this application was spent on the legal policies and protections that need to be involved, starting with defining policies and procedures for

- searching of public postings
- covert research: the use of undercover accounts to gain access to private postings
- undercover investigations: the use of social media to communicate with suspects using an undercover account.

The panel also discussed a general need to help agencies investigate and counter social media– and internet-enabled crimes, such as human trafficking and blackmail.

CORE SECURITY, PRIVACY, AND CIVIL RIGHTS PROTECTIONS

As noted, the panel's deliberations (and this report) are intended to cover not just core applications and use cases for social media and social network analysis but also core protections needed to ensure the appropriate and sustainable application of these technologies in law enforcement. Reflecting the state of development of policy and practice in this area, there was diversity in the views and ideas expressed in the panel discussion, contrasting with the relative consensus around use cases. The following discussion reflects protections identified by one or more panelists either on the questionnaire or during the workshop discussion. This list is not intended as a model policy, although it does represent a set of ideas that could provide a starting point to develop policy.

Assessment framework. Privacy and civil rights panelists suggested a three-part framework for considering the risks of, and organizing the protections needed for, emerging "surveillance" technologies such as social media and social network analysis:

- *Data collection:* What data are being collected, and how?
- *Analysis:* How are the data being analyzed, and what implications does that have? For example, what algorithm is being used, on what data, and what does it look for?
- *Actions:* What do you do with the results? For example, results leading to increased punishment should result in much higher scrutiny than results leading to increased community engagement.

Protections for Data Collection

Protections for data collection relate primarily to documenting procedures and policies, and having protections, for data searches and collections. At the base of these protections are ensuring probable cause for digital searches for investigations. Federal law (28 CFR 23, "Criminal Intelligence Systems Operating Policies") requires that agencies cannot collect information for investigative purposes without criminal predication. There is a general preclusion of searches of First Amendment–protected speech for criminal investigative reasons. Search warrants are needed to access privately posted information. Agencies will need standard procedures for legal process serving to internet service providers and email service providers.

Panelists discussed needs for policies and procedures on criteria for approving long-term, persistent collection of data (i.e., ongoing surveillance in the virtual realm) for both investigative and safety purposes.

Panelists also explored elements of policies and procedures for covert research and undercover investigations. These include conditions for approval; training required on what to do and what not to do; provisions for monitoring and auditing by supervisors; and recording and auditing of methods employed.

Protections for Analytic Activities

Panelists discussed a common set of policies and procedures needed for the deployment and use of analytic tools drawing on social media and other personal communications data, including needs for provisions on

- identifying, credentialing, and actively managing the set of authorized users
- oversight procedures to assess whether authorized usage meets legal and policy guidelines
- oversight of analysis algorithms being employed, including assessing algorithms' functionality, accuracy, and lack of biases along racial and socioeconomic lines
- protections on exports of results procedures, such as requirements for sharing, case management systems being used, and so on
- protection of information, including preventing leaks
- auditing processes to investigate complete trails of usage activity in detail, along with policies and thresholds to determine when audits are performed.

Protections for Actions

Panelists discussed two types of protections they saw as needed when social media data and social network analysis inform law enforcement decisions to take action. The first is to have protections against policing practices being distorted in systematic ways, especially distortions that cause more adverse enforcement actions. These included policies to prevent the desire for more data to drive intervention, such as officers conducting more stops or field interviews due to a perceived need to update a social media or social network analysis database. They also suggested a need for policies to prevent conducting more stops based only on casual social connections that have not been confirmed to be genuine criminal connections by subsequent investigation (both manual and machine-assisted). It was noted that "just because you have 500 Facebook friends doesn't mean you have a real relationship with more than a few of them." As

a result, action being driven solely by an individual having one "bad guy" among his or her 500 connections was not viewed as appropriate.

The second was to have policies to govern how to make decisions about interventions consistently and in an unbiased manner. For interventions such as focused deterrence informed by social media data or social network analysis, these include deciding what to do with those "at risk" consistently, accounting for whether the person is a high threat to the community versus at high risk of being a victim. Consistent criteria to guide the decision whether to "provide help" or "prosecute fully" when individuals are identified as high risk would help minimize the potential for these new data streams to reinforce or even create new sources of bias in justice decisionmaking.

NEEDS FOR INNOVATION

Informed by the business cases and discussion of the types of protections merited for these types of data and analytical approaches, the panel turned to the identification of needs related to social media and social network analysis application in law enforcement. As a result of that discussion, the expert panel collectively identified and prioritized 37 needs. The complete list of needs is presented in Appendix B. Twenty-two of these needs met our criteria for being priority needs. These 22 could be logically grouped under four themes. (Appendix A describes the full technical methods for generating needs, prioritizing them, and grouping the priority needs into themes.)

Theme 1: Supporting Working with Communities to Develop Policies and Strategies for Using Social Media and Social Network Analysis

The panel's first theme calls for a two-part agenda for multi-stakeholder policies and strategies development. The first, *improving how agencies work with community stakeholders on social media and social network analysis issues*, directly informs developing improved policies and strategies for employing these types of analysis. This theme includes developing best practices for discussing uses of social media data and social network analysis with the public, as well as engaging with stakeholders on policy decisions and follow-up actions (Table 2). The theme also includes working with communities to assess specified social media and social network analysis policies, including assessing community councils for deciding on privacy controversies, and assessing what parts of legacy guidance are outdated and how to replace them.

The second part of this theme builds off improved relations with stakeholders to *collectively develop model procedures and policies*. Specific needs here include developing policies for using commercial social media tools, conducting covert social media research, and conducting undercover social media investigations and more broadly pursuing consensus on the tools being used, quality assurance, protections against bias, and civil liberties protections (Table 3).

Theme 2: Supporting Technical Research for Law Enforcement's Use of Social Media and Social Network Analysis

In general, panelists noted that both use and understanding of these types of analysis for law enforcement were in their infancy. Thus, there is an overarching need for research and development on law enforcement applications, including research and evaluation on social media monitoring; social media and social network analysis tools and techniques as applied to law enforcement applications; and tools and techniques supporting search and interoperable data extraction from a full range of social media postings (text, images, video, etc.). See Table 4.

As shown in Figure 9, research and development are needed throughout the social media and social network analysis chain:

- **Getting data.** Panelists noted that it is very difficult to extract data accurately and consistently. There are needs both to assess existing extraction features in social media tools and to develop new tools.
- **Searching data for relevant information.** Panelists indicated that data sets (especially for social media) are often enormous and impractical to review manually. There is a need to develop a search capability tailored to law enforcement needs.
- **Data analysis tools.** Panelists noted needs for technical assessments of current social media analysis, social network analysis, and redaction tools to better understand what could be better employed now and what remains to be developed. Panelists noted that these assessments can start with only baseline descriptions of tools practitioners currently view as useful for particular applications; reflecting this need for knowledge sharing, there was strong

Table 2. Priority Needs to Improve Partnerships with Communities on Social Media and Social Network Analysis Issues

Issue	Need	Comment
There is a lack of public review and discussion of law enforcement policies on social network analysis.	Develop best practices for transparency with regard to use of social network analysis and accompanying data.	Top of Tier 1
There is a lack of public review and discussion of law enforcement policies on social media.	Develop best practices for transparency with regard to use of social media data.	
When analyses provide valuable insights into risk to members of the public, community groups, experts, technologists, and law enforcement should collaborate from the beginning.	Conduct research on best practices with regard to actions taken by practitioners from multiple disciplines when risks are identified.	
There are challenges in balancing transparency, privacy, and judicial fairness in handling digital evidence for criminal justice and public access purposes.	Conduct a review of the efficacy and acceptability of state and local privacy councils (one example is in Oakland, California).	
When analyses provide valuable insights into risk to members of the public, community groups, experts, technologists, and law enforcement should collaborate from the beginning.	Identify the best times and places to engage the community, practitioners, and other experts.	
Best practices and policy guidelines have been published by a variety of organizations over the years in multiple versions, but there is no authoritative way of determining whether an older one has been superseded.	Conduct periodic reviews of existing policies and procedures, with the intention of codifying content and identifying potentially outdated guidance.	

Table 3. Priority Needs to Develop Policies and Procedures

Issue	Need	Comment
There is a lack of standard operating procedures governing use of paid social media tools.	Identify existing policies or develop new model policies (where needed) for using social media tools.	Top of Tier 1
There is a lack of standard operating procedures governing undercover social media investigations (with two-way communication).	Identify existing policies or develop new model policies (where needed) for undercover social media investigations.	Top of Tier 1
There is a lack of standard operating procedures governing covert social media research (without two-way communication).	Identify existing policies or develop new model policies (where needed) for covert social media research.	
When analyses provide valuable insights into risk to members of the public, community groups, experts, technologists, and law enforcement should collaborate from the beginning.	Foster dialogue for an "accountability movement"—get to consensus on tools being used, quality assurance, protections against bias, and civil liberties protections.	

Table 4. Priority Needs for Technical Research and Development

Issue	Need	Comment
Practitioners typically need to extract a unique set of features and alerts (e.g., frequency of contact) from social data (e.g., phones, social media, etc.).	Conduct a gap analysis on existing automated social monitoring tools to determine the shortcomings for criminal justice purposes.	
Often there are several needs to redact video evidence (e.g., discovery, evidence/exhibits, and public/freedom of information).	Conduct a forum for the existing software developers and practitioners/users to exchange information on the shortcomings of existing software.	
There is insufficient information on the efficacy of commercial tools and techniques for social media analysis.	Conduct an independent review of commercial tools and techniques for social media analysis.	
There is insufficient information on the efficacy of commercial tools and techniques for social network analysis.	Conduct an independent review of commercial tools and techniques for social network analysis.	
Social data extraction tools are often not interoperable.	Develop software that performs partial extraction of relevant information in a format that can be easily compared.	High-value, high-risk
When requesting information from social media organizations or collecting it from devices, the resulting data set is often huge (data overload).	Develop easy-to-use, search engine–like functionality for large data sets in a variety of formats (text, images, video, etc.).	High-value, high-risk

Figure 9. Social Media/Social Network Analysis Chain

RAND *RR2301-9*

interest by panel members anytime a tool that worked well for a given purpose was mentioned.

Theme 3: Training for Law Enforcement

Panelists claimed that, in general, available social media and social network analysis training was not well suited for law enforcement. Instead, most existing training was described as product-focused and/or focused on commercial and defense applications, as these have been the principal sectors acquiring social media and social network analysis tools to date. Panelists called for a study of the size and extent of the training "gap," to identify barriers to having tools and training that are genuinely suited for law enforcement, approaches for overcoming them, and a way ahead to conduct the studies, analyses, and educational material development needed to prepare law enforcement–focused materials for social media and social network analysis training. As a short-term training priority, panelists called for developing model training on legal implications, especially constitutional implications, and required protective measures. See Table 5.

Theme 4: A Help Desk for Interacting with Social Media Companies

As a group, panelists felt that the level of cooperation from private-sector companies with law enforcement hindered their ability to find, access, and use the nonpublic social media data needed for specific investigations effectively. (A typical example of data needed would be all postings from a specific person of interest in an investigation, during a specified time of interest.) Panelists ascribed companies' reticence to the costs involved and broader societal concerns about government (particularly federal government) surveillance, but more broadly, as one panelist put it, "almost no customer base wants companies to cooperate with law enforcement—but there are customer bases that want companies [to actively] not cooperate."

As a result, panelists raised a variety of issues about interaction with social media firms, including procedural hurdles (e.g., companies rejecting what the panelist viewed as legal and appropriate data requests), technical barriers (e.g., the practice of cloud data being broken up or "sharded" and stored in different locations, potentially in different countries), and jurisdictional problems (e.g., fighting the provision of

Table 5. Priority Needs for Training

Issue	Need	Comment
There is a lack of legal training on constitutional implications (civil liberties and privacy) and relevant cases.	Develop model training curricula for social media and social media analysis (for all practitioner communities in the criminal justice system).	Top of Tier 1
Existing training is tailored to the intelligence community or private sector rather than law enforcement.	Examine the reach and scalability of existing training and attempt to identify the size and scale of the training "gap."	
Existing trainings are usually conducted by industry and are specific to their tool set.	Examine the reach and scalability of existing training and attempt to identify the size and scale of the training "gap."	

data to a U.S. law enforcement agency because some or all of it is located outside the country). Panelists were also skeptical of being able to negotiate these issues with companies on an agency-by-agency basis. For example, panelists noted that some social media companies consistently chose not to participate in meetings with law enforcement groups, limiting opportunities to build consensus and strengthen collaboration.

Instead, panelists requested funding a "help desk" that would

- help agencies submit process requests that social media companies will not reject, which includes monitoring shifts in the companies' requirements over time and helping agencies submit requests that are sufficiently limited and germane to investigations at hand
- help interpret the results, which includes providing tools to search or analyze data produced in formats that may also change over time
- help submit requests for social media companies to shut down live feeds and posts of violence and safety-threatening activity.

See Table 6.

Table 6. Priority Needs for a Help Desk for Interacting with Social Media Companies

Issue	Need	Comment
Often, "real-time" crimes are streamed live on social media. In such situations, law enforcement needs to be able to quickly inform the site to take down the video.	Explore establishing (and supporting) peer "help desk" experts for practitioners to reach out to in such situations.	
The "data" returned from legal process requests are often unusable or difficult to correlate with existing data.	Establish a help desk–type system whereby investigators can be connected with other investigators who are experts in obtaining and extracting information from particular sources.	
The "data" returned from legal process requests are often unusable or difficult to correlate with existing data.	Establish or fund a liaison that can be a source of knowledge on how to obtain usable information from specific sources (mobile phone companies, social media companies, etc.).	High-value, high-risk

SUMMARY AND CONCLUSIONS: THE INNOVATION AGENDA FOR SOCIAL MEDIA AND SOCIAL NETWORK ANALYSIS IN LAW ENFORCEMENT

What to Do and Not Do with Social Media and Social Network Analysis in Law Enforcement

Reflecting both the five business cases that the panelists identified for the use of social media and social network analysis data and tools and the core elements required to protect citizens' constitutional rights, the expert panel identified and prioritized a set of needs that provide an innovation agenda to better support the use of these types of analysis in law enforcement. Although time-critical situations, such as responding to violent activities in progress, have distinct issues from longer-term usage of these tools in investigative applications, the needs identified showed common issues of policy and practice that reached across the different business cases. These issues, falling in the themes that define the innovation agenda (Figure 10), represent a set of priorities to support the appropriate and sustainable use of these tools for public safety purposes.

The first part of the panelists' innovation agenda (Theme 1) is to support working with communities to develop policies and strategies for using social media and social network analysis. Here, the initial recommendations relate to developing and disseminating best practices for transparency and collaborative decisionmaking for employing social media and social network analysis technologies, as well as collaboratively creating a series of model policies for employment and security of social media and social network analysis data.

The second part of the agenda (Theme 2) is technical research on law enforcement–specific social media and social network analysis. As noted, such development is needed because most work to date is commercial- or defense-related. The initial recommendation here is to assess the capabilities of current tools and how they might be better tailored to law enforcement; as a first step of that assessment, create and disseminate a market survey of what tools are being found useful by practitioners now.

Figure 10. The Innovation Agenda

RAND *RR2301-10*

The third part of the agenda (Theme 3) is supporting law enforcement–specific training on social media and social network analysis. Here, the initial recommendations are to develop requirements for training and assess gaps between current (commercial- and defense-focused) training and what is needed for law enforcement–focused training. As noted, training on legal implications and protections is a short-term need that can be addressed by developing a model curriculum.

The final part of the panel's agenda (Theme 4) is to develop a help desk that will help law enforcement agencies navigate requests to social media companies. The help desk would help agencies with making process requests more likely to result in data returns and/or content takedowns that address the needs of specific cases; it would also help agencies process and interpret the data returned from process requests.

APPENDIX A. TECHNICAL SUPPLEMENT

Generating Needs for Innovation

Prior to the workshop, RAND sent a questionnaire to the expert panelists, asking them to identify the following:

- specific questions that they want social media and social network analysis tools to be able to answer; specific questions that the tools should not answer (because of technology challenges, the potential for information overload, or the potential to violate privacy and civil rights)
- specific security, privacy, and civil rights protections that the social media and social network investigative processes need to have throughout, in terms of specific activities, procedures, and tools and functions
- building on the above, specific *issues*, which are problems or opportunities in the areas of
  - people: educational materials, training
  - process: business processes and policies for using and securing these tools
  - technology: requirements to improve the tools
  - organization: recommendations on parties that should participate and supporting organizational structures.

All the questions, protections, and issues raised were added to an Excel worksheet.

During discussions, panelists were first invited to add additional questions, protections, and issues over what came in on the questionnaire. They were also invited to add details as needed.

The panelists were then invited to identify potential innovations (ways ahead) to address those issues, whether to fix a problem or take advantage of an opportunity. These innovations were calls for specific actions to address the problem or opportunity, and could relate to technological, governmental, policy, or business model innovations. Each need, therefore, includes one issue (problem or opportunity) and one specific innovation to address that issue.

Prioritizing Needs

Panelists rated each need for two measures: potential importance to law enforcement if the need could be successfully addressed, and the likelihood of success (in general). Each panelist rated each need on scales from 1 to 9 (1 low, 9 high). Importance was bracketed as 1 equaling virtually no benefit to law enforcement, and 9 equaling the same benefit of prior "game-changing" technologies, such as body armor and crime hot spot analysis. Likelihood of success was bracketed as 1 equaling about a 10 percent chance of success and 9 equaling about a 90 percent chance of success.

To combine the two scores, we took an *expected value (EV)* approach, multiplying the two scores from each participant together to come up with a single EV score that reflects, in words, the average amount of benefit law enforcement could expect to see from investing in addressing a given need. We then took the median of the EV scores from all panelists to get an EV score for each need. We used the median score because it is both robust to outliers and does not presume any underlying probability distributions for the panelists' ratings.

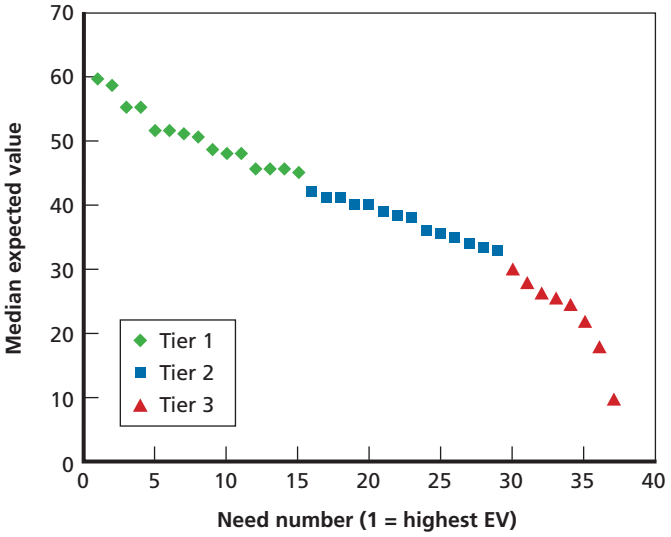
EV approaches are fundamental in assessing choices under uncertainty (see, for example, de Neufville, 1990, pp. 312–313). This approach has been used in prior RAND research on criminal justice technology needs, including the first and second Law Enforcement Advisory Panels, which were broad-based surveys of needs for law enforcement (Hollywood et al., 2015, 2017). It has also been used on prior broad-based studies of corrections and courts needs (Jackson et al., 2015, 2016), as well as broadband communications needs for law enforcement (Hollywood et al., 2016).

We divided the needs by median EV score into three priority tiers using a clustering algorithm. We used a hierarchical clustering algorithm employing Ward's, or spherical, clustering rule (Ward, 1963; Murtagh, 1985) to divide the needs into tiers, via the "hclust" package in the R statistical environment, called using both native R code and the Wessa statistical web portal (Wessa, 2012). Figure A.1 plots the needs' median EV scores by priority tier.

Hierarchical clustering generates a *dendrogram*, which graphically shows which data points are mathematically closest together. Points (in this case, needs' EV scores) that are very close tend to be on the same low-level twig. Larger groups of points that are also broadly similar are on larger "branches." One can divide points into a set number of clusters by taking the points on each of the highest-level branches ("limbs") to be a cluster. Figure A.2 shows the dendrogram and resulting clusters ("top limbs") resulting from applying hierarchical clustering to the needs' EV scores. In our case, we take the three tiers to be the three groups of needs on each of the three highest branches in the dendrogram, as shown in Figure A.2.

Four needs were in the top sub-branch of the Tier 1 cluster, and can be thought of as the "top of tier 1."

Figure A.1. Plots of Needs' Median Expected Values, by Tiers



RAND *RR2301-A.1*

We checked whether any of the median EV scores constituted a statistical outlier (using the GraphPad calculator [2017], which applies the extreme studentized deviate test). No needs were found to be an outlier.

Priority needs satisfied any of the three following criteria:

- Need in Tier 1 (from hierarchical clustering).
- Need in Tier 2 but had *high importance* (median potential importance at 8 or higher). These can be thought of as "high-risk, high-reward" needs.
- Need in Tier 2 but had same or greater median ratings for individual measures as other Tier 1 needs. This set includes one need that had an identical solution statement to another Tier 1 need—just a different motivating problem statement.

We also checked to see whether there were any "low-hanging fruit" needs, defined as being in Tier 2 but having a very low risk (median likelihood of success score of 8 or higher). There were no such needs in this study.

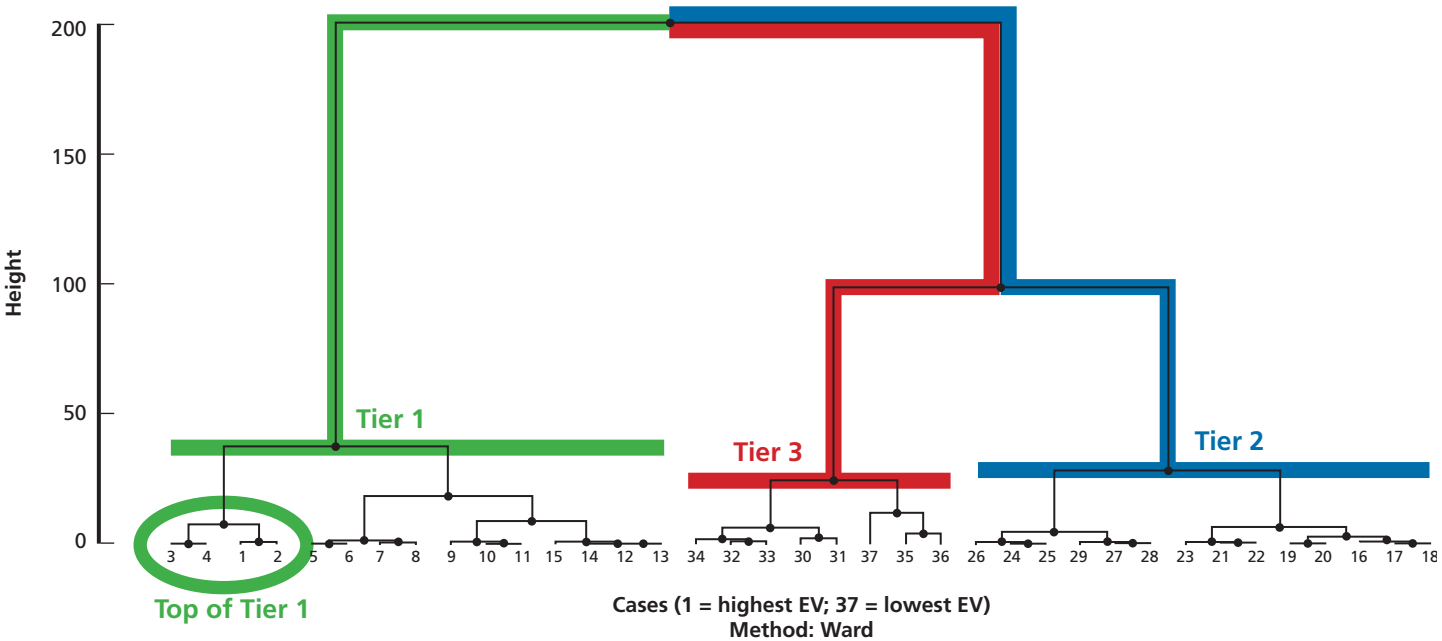
There are 22 priority needs. Figure A.3 shows that a plot of the needs' median likelihood and importance scores results in all priority needs falling into a triangle on the upper right corner of the graph.

Identifying Themes

To identify top themes reflecting groups of needs, we performed a network analysis to identify groups of needs. In this analysis, we coded that a link exists between needs if those needs concern the same type of issue or proposed solution (proposed way ahead). Figure A.4 shows the matrix of links between the priority needs.

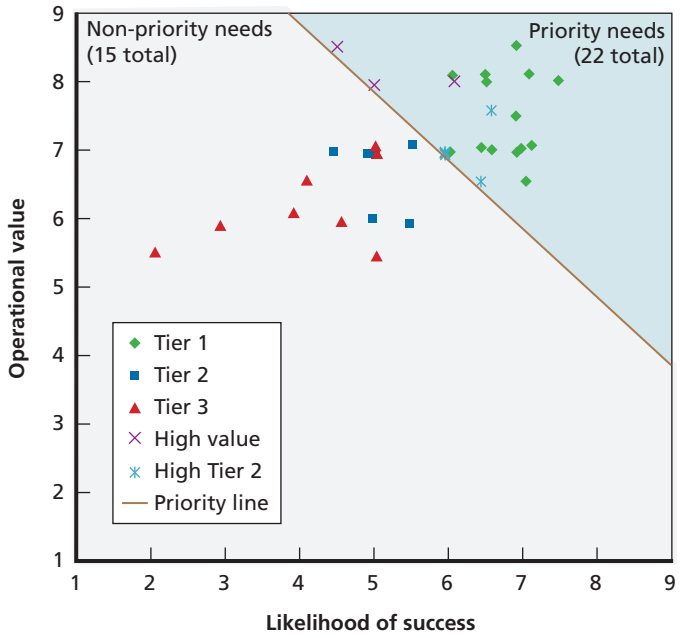
The resulting network graph of the needs and their links is shown in Figure A.5. As shown, the needs fell into four disjoint groups. The similarities between the needs in each group implied an overarching theme for each group, also shown in Figure A.5.

Figure A.2. Dendrogram of Social Media/Social Analysis Needs (from Hierarchical Clustering)



RAND *RR2301-A.2*

Figure A.3. Plot of the 37 Needs by Median Likelihood of Success and Median Operational Value



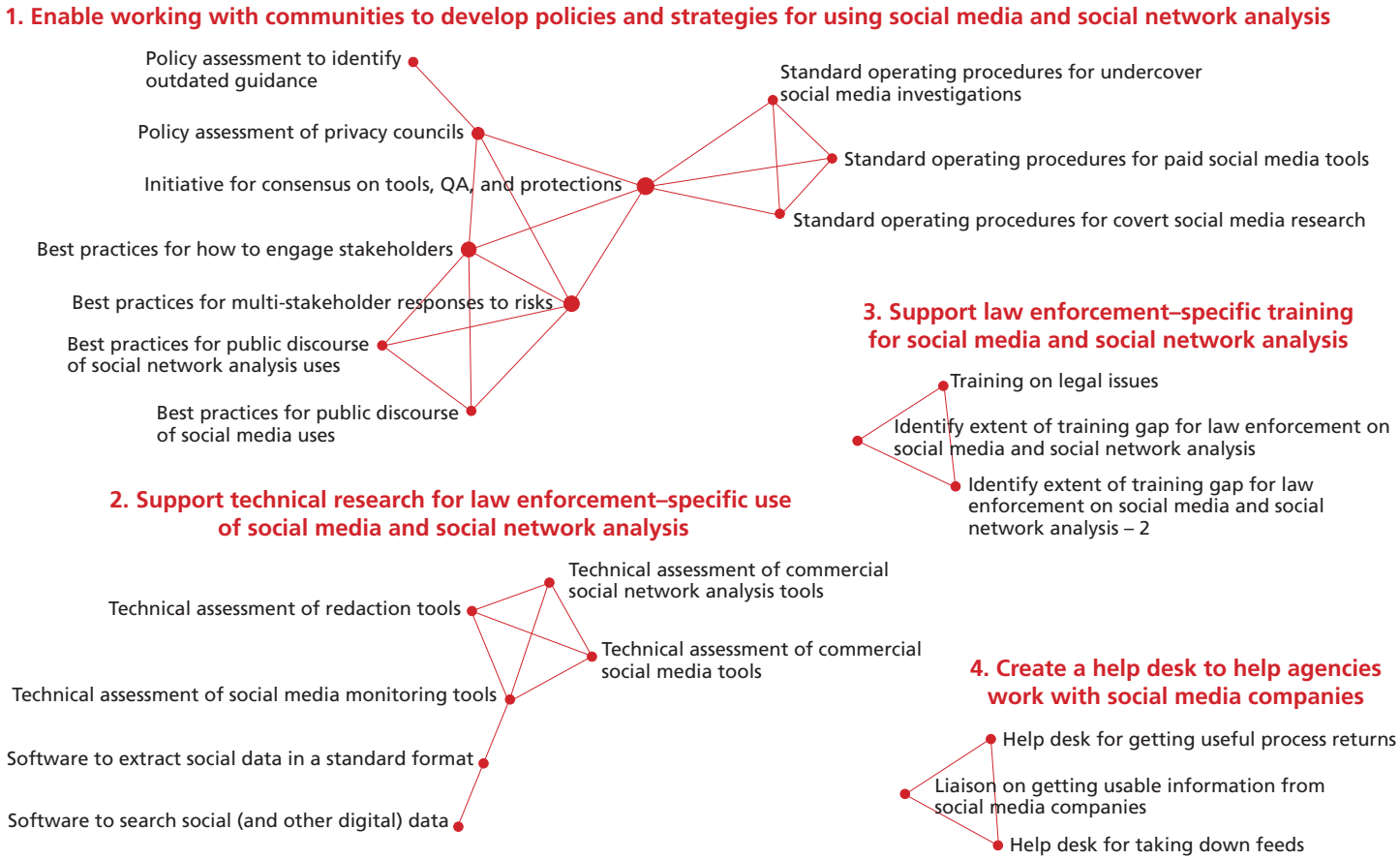
RAND *RR2301-A.3*

Figure A.4. Similarity Links Between the 22 Priority Needs

	SOP for paid SM tools	BP for public discourse of SNA uses	SOP for undercover SM investiga-tions	Training on legal issues	Tech assessment of SM monitoring tools	Help desk for taking down feeds	SOP for covert SM research	BP for public discourse of SM uses	BP for multi-stakeholder responses to risks	Policy assessment of privacy councils	…
SOP for paid SM tools	0	0	1	0	0	0	1	0	0	0	
BP for public discourse of SNA uses	0	0	0	0	0	0	0	1	1	0	
SOP for undercover SM investigations	1	0	0	0	0	0	1	0	0	0	
Training on legal issues	0	0	0	0	0	0	0	0	0	0	
Tech assessment of SM monitoring tools	0	0	0	0	0	0	0	0	0	0	
Help desk for taking down feeds	0	0	0	0	0	0	0	0	0	0	
SOP for covert SM research	1	0	1	0	0	0	0	0	0	0	
BP for public discourse of SM uses	0	1	0	0	0	0	0	0	1	0	
BP for multi-stakeholder responses to risks	0	1	0	0	0	0	0	1	0	1	
Policy assessment of privacy councils	0	0	0	0	0	0	0	0	1	0	
BP for how to engage stakeholders	0	1	0	0	0	0	0	1	1	1	
Tech assessment of redaction tools	0	0	0	0	1	0	0	0	0	0	
Policy assessment to ID outdated guidance	0	0	0	0	0	0	0	0	0	1	
ID extent of training gap for LE on SM/SNA	0	0	0	1	0	0	0	0	0	0	
…											

RAND *RR2301-A.4*

Figure A.5. Distinct Groups of Needs and Their Unifying Themes



RAND *RR2301-A.5*

APPENDIX B. COMPLETE LIST OF NEEDS

Table B.1. Priority Needs to Improve Partnerships with Communities on Social Media and Social Network Analyis Issues

Issue	Need	Comment
There is a lack of public review and discussion of law enforcement policies on social network analysis.	Develop best practices for transparency with regard to use of social network analysis and accompanying data.	Top of Tier 1
There is a lack of public review and discussion of law enforcement policies on social media.	Develop best practices for transparency with regard to use of social media data.	
When analyses provide valuable insights into risk to members of the public, then community groups, experts, technologists, and law enforcement should collaborate from the beginning.	Conduct research on best practices with regard to actions taken by practitioners from multiple disciplines when risks are identified.	
There are challenges in balancing transparency, privacy, and judicial fairness in handling digital evidence for criminal justice and public access purposes.	Conduct a review of the efficacy and acceptability of state and local privacy councils (one example is in Oakland, California).	
When analyses provide valuable insights into risk to members of the public, then community groups, experts, technologists, and law enforcement should collaborate from the beginning.	Identify the best times and places to engage the community, practitioners, and other experts.	
Best practices and policy guidelines are published by a variety of organizations over the years in multiple versions, but there is no authoritative way of determining when an older one is superseded.	Conduct periodic reviews of the existing policy and procedure with the intention of codifying content and identifying potentially outdated guidance.	

Table B.2. Priority Needs to Develop Policies and Procedures

Issue	Need	Comment
There is a lack of standard operating procedures governing use of paid social media tools.	Identify existing policies or develop new model policies (where needed) for using social media tools.	Top of Tier 1
There is a lack of standard operating procedures governing undercover social media investigations (with two-way communication).	Identify existing policies or develop new model policies (where needed) for undercover social media investigations.	Top of Tier 1
There is a lack of standard operating procedures governing covert social media research (without two-way communication).	Identify existing policies or develop new model policies (where needed) for covert social media research.	
When analyses provide valuable insights into risk to members of the public, community groups, experts, technologists, and law enforcement should collaborate from the beginning.	Foster dialogue for an "accountability movement"—get to consensus on tools being used, quality assurance, protections against bias, and civil liberties protections.	

Table B.3. Priority Needs for Technical Research and Development

Issue	Need	Comment
Practitioners typically need to extract a unique set of features and alerts (e.g., frequency of contact) from social data (e.g., phones, social media, etc.).	Conduct a gap analysis on existing automated social monitoring tools to determine the shortcomings for criminal justice purposes.	
Often there are several needs to redact video evidence (e.g., discovery, evidence/exhibits, and public/freedom of information).	Conduct a forum for the existing software developers and practitioners/users to exchange information on the shortcomings of existing software.	
There is insufficient information on the efficacy of commercial tools and techniques for social media analysis.	Conduct an independent review of commercial tools and techniques for social media analysis.	
There is insufficient information on the efficacy of commercial tools and techniques for social network analysis.	Conduct an independent review of commercial tools and techniques for social network analysis.	
Social data extraction tools are often not interoperable.	Develop software that performs partial extraction of relevant information in a format that can be easily compared.	High-value, high-risk
When requesting information from social media organizations or collecting it from devices, the resulting data set is often huge (data overload).	Develop easy to use, search engine–like functionality for large data sets in a variety of formats (text, images, video, etc.).	High-value, high-risk

Table B.4. Priority Needs for Training

Issue	Need	Comment
There is a lack of legal training on constitutional implications (civil liberties and privacy) and relevant cases.	Develop model training curricula for social media and social network analysis (for all practitioner communities in the criminal justice system).	Top of Tier 1
Existing training is tailored to the defense community or the private sector rather than law enforcement.	Examine the reach and scalability of existing training and attempt to identify the size and scale of the training "gap."	
Existing trainings are usually conducted by industry and are specific to their tool set.	Examine the reach and scalability of existing training and attempt to identify the size and scale of the training "gap."	

Table B.5. Priority Needs for a Help Desk for Interacting with Social Media Companies

Issue	Need	Comment
Often, "real-time" crimes are streamed live on social media. In such situations, law enforcement needs to be able to quickly inform the site to take down the video.	Explore establishing (and supporting) peer "help desk" experts for practitioners to reach out to in such situations.	
The "data" returned from legal process requests are often unusable or difficult to correlate with existing data.	Establish a help desk–type system whereby investigators can be connected with other investigators who are experts in obtaining and extracting information from particular sources.	
The "data" returned from legal process requests are often unusable or difficult to correlate with existing data.	Establish or fund a liaison that can be a source of knowledge on how to obtain usable information from specific sources (e.g., mobile phone companies, social media companies).	High-value, high-risk

Table B.6. Other Needs from the Social Media/Social Network Analysis Workshop

Issue	Need	Comment
There are not enough social network analysis practitioners to meet the demand.	Conduct research into the gaps between where the profession is now and where it should be.	Tier 2
Often there are several needs to redact video evidence (e.g., discovery, evidence/exhibits, and public/freedom of information).	Develop a standard policy for what and how to redact.	Tier 2
When social network analysis is successful at identifying individuals at risk, law enforcement often has difficulty finding an appropriate way to share those insights.	Develop best practices for sharing information with individuals and multidisciplinary organizations (e.g., social support organizations)	Tier 2
When relocation information is obtained, the algorithm that was used (GPS, Wi-Fi/cell triangulation) and the level of accuracy is often unknown (and cannot be obtained from the company because it is proprietary).	Conduct research and interviews with industry organizations to identify ways to address this issue.	Tier 2
The "data" returned from legal process requests are often unusable or difficult to correlate with existing data.	Establish (and require compliance with) a standard for structuring certain types of information in response to legal process requests (this has more or less occurred with cellular carrier data).	Tier 2
It is difficult to determine the most appropriate broadness or narrowness of scope for an electronic records request (e.g., requesting Google's records for a unique search two weeks before an event within a town of 25,000).	Conduct research on best practices and publish with appropriate case story vignettes.	Tier 2
When evidence or data are delivered, there isn't a readily available index or table of contents to point investigators/prosecution to the most important and relevant items.	Develop a set of metadata descriptions for typical evidence types that are obtained from devices and organizations.	Tier 2
There are challenges in balancing transparency, privacy, and judicial fairness in handling digital evidence for criminal justice and public access purposes.	Conduct a review of state and local freedom of information laws and policies to determine appropriateness for redaction of new technologies such as body-worn camera video.	Tier 3
The "data" returned from legal process requests are often unusable or difficult to correlate with existing data.	Establish a database that can be a source of knowledge on how to obtain usable information from specific sources (mobile phone companies, social media companies, etc.).	Tier 3
Social network analysis algorithms don't support cross-checking.	Develop or identify tools that can compare patterns identified in internal law enforcement data with patterns identified in social media data.	Tier 3
Crimes are often "reported" by sharing text, photos, or video on social media or directly with law enforcement. In such situations, geolocation or entity resolution (who is in the picture, etc.) is difficult.	Develop or identify tools (software or services) that can identify geographic features in images and correlate them with known locations, individuals, etc. (TrafficCam.com and Griffeye have some of this functionality.)	Tier 3
Social network analysis tools and geographic information system tools often do not interoperate very well.	Conduct research on best practices for conducting analyses using both types of analysis (and potentially identify gaps in functionality).	Tier 3

Table B.6—continued

Issue	Need	Comment
Accurately extracting meaning from social media communications is difficult because language and style is dynamic and constantly changing.	Conduct research to identify the appropriate amount of knowledgeable interpretation and validation when making "automated" decisions.	Tier 3
Lack of social media companies being involved may lead to increased efforts to block investigative tools—e.g., concerns about internet service providers and email service providers taking actions to evade search warrants.	Conduct or facilitate an "industry exchange" where the companies and state and local agencies can better understand each other.	Tier 3
In emergencies where a life is threatened, social media companies should be compelled to provide the information requested by law enforcement (e.g., the "2703" exemption language should be changed from "may" to "shall"). If the emergency request is not in good faith, there should be appropriate sanctions against the officer or the officer's agency.	Conduct research and interviews to examine the feasibility and acceptability of modifications to the law.	Tier 3

REFERENCES

Adolph, Steve, Alistair Cockburn, and Paul Bramble, *Patterns for Effective Use Cases*, Boston, Mass.: Addison-Wesley Longman Publishing Co., Inc., 2002.

Ahajjam, Sara, Mohamed El Haddad, and Hassan Badir, "A New Scalable Leader-Community Detection Approach for Community Detection in Social Networks," *Social Networks*, Vol. 54, July 2018, pp. 41–49.

Bichler, Gisela, and Aili Malm, eds., *Disrupting Criminal Networks: Network Analysis in Crime Prevention*, Boulder, Colo.: FirstForumPress, 2015.

Braga, Anthony A., Brandon C. Welsh, and Cory Schnell, "Can Policing Disorder Reduce Crime? A Systematic Review and Meta-Analysis," *Journal of Research in Crime and Delinquency*, Vol. 52, No. 4, 2015, pp. 567–588. As of June 5, 2018: http://petermoskos.com/files/BW/Braga_2015_policing_disorder_reduces_crime.pdf

Cheung, Jason, and Ryan Prox, Vancouver Police Department, "Fighting Crime with CRIME: A Single, Integrated Analytical and Investigative Umbrella," presentation to the International Association of Chiefs of Police Law Enforcement Information Management Conference, Indianapolis, Ind., May 23, 2012.

City of Oakland, California, "Privacy Advisory Commission,'" webpage, 2017. As of July 10, 2017: http://www2.oaklandnet.com/government/o/CityAdministration/d/PrivacyAdvisoryCommission/index.htm

Coldren, James, and John Markovic, "Utilizing Social Network Analysis to Reduce Violent Crime," Violence Reduction Network Webinar Series, July 20, 2015.

de Neufville, R., *Applied Systems Analysis: Engineering Planning and Technology Management*, New York: McGraw-Hill, 1990.

Dughi, Paul, "17 Times Social Media Helped Police Track Down Thieves, Murderers, and Gang Criminals," *Medium: The Mission*, June 25, 2016. As of November 20, 2017: https://medium.com/the-mission/17-times-social-media-helped-police-track-down-thieves-murderers-and-gang-criminals-a814b6c40fb

Fox, Andrew, Kenneth Novak, Joe McHale, and Andries Zylstra, "Research in Brief: Incorporating Social Network Analysis into Policing," *The Police Chief*, Vol. 81, December 2014, p. 16. As of November 2, 2017: http://www.policechiefmagazine.org/research-in-brief-incorporating-social-network-analysis-into-policing/

Girvan, M., and M. E. J. Newman, "Community Structure in Social and Biological Networks," *Proceedings of the National Academy of Sciences*, Vol. 99, No. 12, June 11, 2002.

Green, Ben, Thibaut Horel, and Andrew V. Papachristos, "Modeling Contagion Through Social Networks to Explain and Predict Gunshot Violence in Chicago, 2006 to 2014," *JAMA Internal Medicine*, Vol. 177, No. 3, 2017, pp. 326–333.

Hannemann, Robert A., and Mark Riddle, *Introduction to Social Network Methods*, Riverside, Calif.: University of California, Riverside, 2005. As of June 10, 2017: http://faculty.ucr.edu/~hanneman/

Herman, B., and J. M. Siegelaub, "Is This Really Worth the Effort? The Need for a Business Case" (paper presented at PMI® Global Congress 2009—North America, Orlando, Fla.), Newtown Square, Pa.: Project Management Institute, 2009. As of June 9, 2017: https://www.pmi.org/learning/library/need-business-case-6730

Hollywood, John S., John E. Boon, Jr., Richard Silberglitt, Brian G. Chow, and Brian A. Jackson, *High-Priority Information Communications Technology Needs for Law Enforcement*, Santa Monica, Calif.: RAND Corporation, RR-737-NIJ, 2015. As of June 12, 2015: http://www.rand.org/pubs/research_reports/RR737.html

Hollywood, John S., Dulani Woods, Sean E. Goodison, Andrew Lauland, Lisa Wagner, Thomas J. Wilson, and Brian A. Jackson, *Fostering Innovation in U.S. Law Enforcement: Identifying High-Priority Technology and Other Needs for Improving Law Enforcement Operations and Outcomes*, Santa Monica, Calif.: RAND Corporation, RR-1814-NIJ, 2017. As of June 26, 2018: https://www.rand.org/pubs/research_reports/RR1814.html

Hollywood, John S., Dulani Woods, Andrew Lauland, Sean E. Goodison, Thomas J. Wilson, and Brian A. Jackson, *Using Future Broadband Communications Technologies to Strengthen Law Enforcement*, Santa Monica, Calif.: RAND Corporation, RR-1462-NIJ, 2016. As of July 10, 2017: http://www.rand.org/pubs/research_reports/RR1462.html

Hollywood, John S., Dulani Woods, Andrew Lauland, Brian A. Jackson, and Richard Silberglitt, *Addressing Emerging Trends to Support the Future of Criminal Justice: Findings of the Criminal Justice Technology Forecasting Group*, Santa Monica, Calif.: RAND Corporation, RR-1987-BJA, 2018. As of June 11, 2018: https://www.rand.org/pubs/research_reports/RR1987.html

Jackson, Brian A., Duren Banks, John S. Hollywood, Dulani Woods, Amanda Royal, Patrick W. Woodson, and Nicole J. Johnson, *Fostering Innovation in the U.S. Court System: Identifying High-Priority Technology and Other Needs for Improving Court Operations and Outcomes*, Santa Monica, Calif.: RAND Corporation, RR-1255-NIJ, 2016. As of July 2, 2018: https://www.rand.org/pubs/research_reports/RR1255.html

Jackson, Brian A., Joe Russo, John S. Hollywood, Dulani Woods, Richard Silberglitt, George B. Drake, John S. Shaffer, Mikhail Zaydman, and Brian G. Chow, *Fostering Innovation in Community and Institutional Corrections: Identifying High-Priority Technology and Other Needs for the U.S. Corrections Sector*, Santa Monica, Calif.: RAND Corporation, RR-820-NIJ, 2015. As of July 2, 2018: https://www.rand.org/pubs/research_reports/RR820.html

Johnson, Jennifer A., John David Reitzel, Bryan F. Norwood, David M. McCoy, D. Brian Cummings, and Renee R. Tate, "Social Network Analysis: A Systematic Approach for Investigating," *FBI Law Enforcement Bulletin*, March 5, 2013. As of June 12, 2017: https://leb.fbi.gov/articles/featured-articles/social-network-analysis-a-systematic-approach-for-investigating

LexisNexis Risk Solutions, *Social Media Use in Law Enforcement: Crime Prevention and Investigative Activities Continue to Drive Usage*, 2014. As of June 11, 2018: https://www.lexisnexis.com/risk/downloads/whitepaper/2014-social-media-use-in-law-enforcement.pdf

Murtagh, F., *Multidimensional Clustering Algorithms*, Compstat Lectures, Vienna: Physika Verlag, 1985.

National Network for Safe Communities, *Group Violence Intervention: An Implementation Guide*, Washington, D.C.: Office of Community Policing Services, 2016. As of April 10, 2018: https://nnscommunities.org/uploads/GVI_Guide_2016.pdf

National Telecommunications and Information Administration, "Next Generation 911," NTIA.doc.gov, January 2017. As of July 10, 2017: https://www.ntia.doc.gov/category/next-generation-911

Papachristos, Andrew V., Christopher Wildeman, and Elizabeth Roberto, "Tragic, but Not Random: The Social Contagion of Nonfatal Gunshot Injuries," *Social Science and Medicine*, Vol. 125, January 2015, pp. 139–150.

Paulo, Damon, Bradley Fischl, Tanya Markow, Michael Martin, and Paulo Shakarian, "Social Network Intelligence Analysis to Combat Street Gang Violence," *Proceedings of the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM '13)*, 2013, pp. 1042–1049. As of April 9, 2018: https://arxiv.org/pdf/1306.6834.pdf

Pew Research Center, "How We Analyzed Twitter Social Media Networks with NodeXL," 2014. As of June 10, 2017: http://www.pewinternet.org/files/2014/02/How-we-analyzed-Twitter-social-media-networks.pdf

Popper, Ben, "How the NYPD Is Using Social Media to Put Harlem Teens Behind Bars: The Untold Story of Jelani Henry, Who Says Facebook Likes Landed Him in Rikers," *The Verge*, December 10, 2014. As of July 10, 2017: https://www.theverge.com/2014/12/10/7341077/nypd-harlem-crews-social-media-rikers-prison

Scott, John, *Social Network Analysis*, Thousand Oaks, Calif.: Sage, 2012.

Social Media Research Foundation, "NodeXL Feature Overview," Smrfoundation.org, 2016. As of June 10, 2017: http://www.smrfoundation.org/nodexl/features/

Ward, J. H., Jr., "Hierarchical Grouping to Optimize an Objective Function," *Journal of the American Statistical Association*, Vol. 58, No. 301, 1963, pp. 236–244.

Wessa, P., Free Statistics Software, Office for Research Development and Education, version 1.2.1, 2018. As of June 26, 2018: https://www.wessa.net/

Acknowledgments

The authors would like to acknowledge the participation and assistance of the panelists of the 2017 Social Media and Social Network Analysis Workshop. We would also like to acknowledge the contributions of Stephen Schuetz, Christopher Rigano, and William Ford of the National Institute of Justice (NIJ), as well as the peer reviewers of the report: Luke Matthews of the RAND Corporation, Aili Malm of the California State University at Long Beach, and anonymous reviewers selected by NIJ.

The RAND Justice Policy Program

The research reported here was conducted in the RAND Justice Policy Program, which spans both criminal and civil justice system issues, with such topics as public safety, effective policing, police-community relations, drug policy and enforcement, corrections policy, use of technology in law enforcement, tort reform, catastrophe and mass-injury compensation, court resourcing, and insurance regulation. Program research is supported by government agencies, foundations, and the private sector.

This program is part of RAND Justice, Infrastructure, and Environment, a division of the RAND Corporation dedicated to improving policy- and decisionmaking in a wide range of policy domains, including civil and criminal justice, infrastructure protection and homeland security, transportation and energy policy, and environmental and natural resource policy.

Questions or comments about this report should be sent to the project leader, Brian A. Jackson at Brian_Jackson@rand.org. For more information about the Justice Policy Program, see www.rand.org/jie/justice-policy or contact the director at justice@rand.org.

About This Report

On behalf of the U.S. Department of Justice, National Institute of Justice (NIJ), the RAND Corporation, in partnership with the Police Executive Research Forum (PERF), RTI International, and the University of Denver, is carrying out a research effort to assess and prioritize technology and related needs across the criminal justice community. This initiative is a component of the National Law Enforcement and Corrections Technology Center (NLECTC) System and is intended to support innovation within the criminal justice enterprise. For more information about the NLECTC Priority Criminal Justice Technology Needs Initiative, see www.rand.org/jie/justice-policy/projects/priority-criminal-justice-needs.

This report is one product of that effort. It summarizes an expert panel convened by the National Institute of Justice in April 2017 to identify high-priority needs for law enforcement's use of social media and social network analysis.

The panel characterized business cases for employing social media and social network analysis in law enforcement, including monitoring for short-term safety threats in postings; identifying those at high risk of involvement in violence, either acutely or chronically; and investigating specific crimes and organized crime networks. The panel also specified a core case not to do: monitoring of First Amendment–protected activity for vague purposes.

The panel next specified a framework for providing computer security, privacy, and civil rights protections when employing these types of analysis. The framework includes data protections for ensuring legal backings and information security; analytic protections for ensuring protection of findings, legal backing, and equitable justice outcomes; and protections on enforcement actions to ensure consistent and equitable actions and outcomes.

Finally, the panel identified and prioritized needs for innovation related to social media and social network analysis. The first part of the resulting innovation agenda concerns developing policies and strategies, including best practices for transparency and collaborative decisionmaking with communities, as well as model policies. The second part is technical development, starting with assessing current tools and how they might be better tailored to law enforcement. The third part concerns law enforcement–specific training, starting with assessing gaps in current training. Training on legal issues is a short-term priority. The final part is creation of a help desk to help law enforcement agencies navigate requests to social media companies and interpret the resulting data.

Mentions of products do not represent approval or endorsement by the National Institute of Justice or the RAND Corporation.

NIJ | National Institute of Justice
STRENGTHEN SCIENCE. ADVANCE JUSTICE.

This publication was made possible by Award Number 2013-MU-CX-K003, awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect those of the Department of Justice.

Limited Print and Electronic Distribution Rights

www.rand.org

RAND CORPORATION

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. **RAND**® is a registered trademark.

RR-2301-NIJ