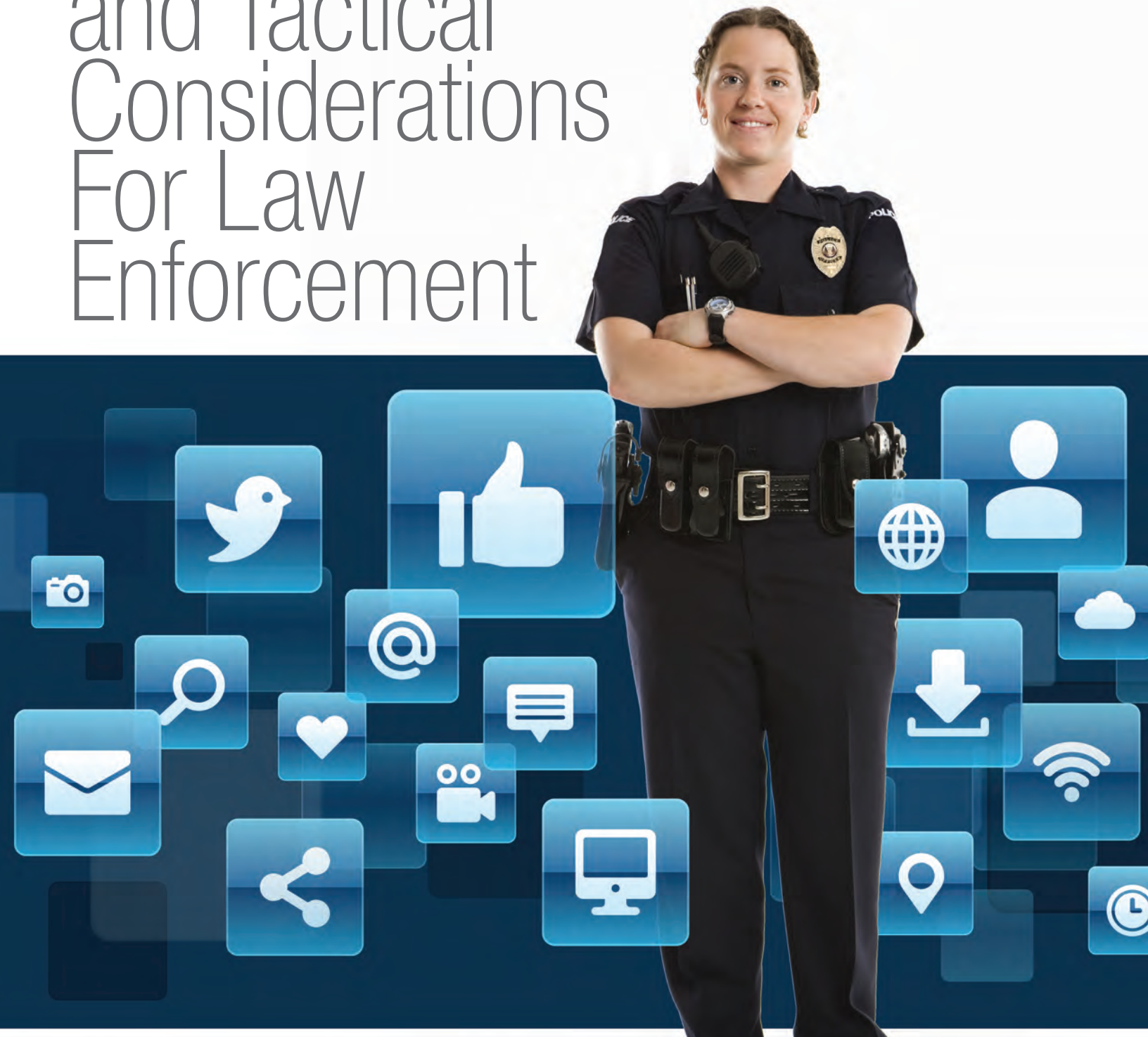
Social Media and Tactical Considerations For Law Enforcement



COPS
Community Oriented Policing Services
U.S. Department of Justice

Police Executive Research Forum

This project was supported by Cooperative Agreement Number 2011-CK-WX-K016 awarded by the Office of Community Oriented Policing Services, U.S. Department of Justice. The opinions contained herein are those of the author(s) and do not necessarily represent the official position or policies of the U.S. Department of Justice. References to specific agencies, companies, products, or services should not be considered an endorsement by the author(s) or the U.S. Department of Justice. Rather, the references are illustrations to supplement discussion of the issues.

The Internet references cited in this publication were valid as of the date of this publication. Given that URLs and websites are in constant flux, neither the author(s) nor the COPS Office can vouch for their current validity.

ISBN: 978-1-932582-72-7

e011331543

May 2013

A joint project of:

COPS
Community Oriented Policing Services
U.S. Department of Justice

POLICE EXECUTIVE RESEARCH FORUM

U.S. Department of Justice
Office of Community Oriented Policing Services
145 N Street, N.E.
Washington, DC 20530

Police Executive Research Forum
1120 Connecticut Avenue, N.W.
Suite 930
Washington, DC 20036

To obtain details on COPS Office programs,
call the COPS Office Response Center at 800-421-6770.

Visit COPS Online at www.cops.usdoj.gov.

Contents

Foreword

The COPS Office and the Police Executive Research Forum are pleased to offer this report on the use of social media in policing.

This report is part of a COPS Office series titled "Emerging Issues in Policing," which is a very appropriate heading for a discussion of social media. The use of social media is a relatively new phenomenon in policing. Many police departments are experimenting with social media—and we emphasize the word "experimenting." Some departments are using social media far more extensively than others, and development of formal policy on social media is generally lagging behind practice. A variety of legal, civil rights, and privacy-related issues regarding social media have been raised, but these issues are nowhere near the point of resolution in the courts yet.

Many departments' initial efforts to use social media platforms such as Facebook and Twitter have been for the purpose of disseminating information to the public about crime issues, crime prevention programs, and police department activities. Chapter 1 of this report describes the social media strategy of the Toronto Police Service, which has one of the most advanced social media programs in existence for disseminating information to the public.

There has been much less discussion of police use of social media for other purposes, such as preventing and investigating crimes, in which the police are gathering information rather than disseminating information. That is the subject of the bulk of this report. We brought together some of the police officials who have been taking the lead in exploring these issues and developing social media programs, and asked them to tell us what they have learned from the successes they have achieved as well as the challenges they have overcome.

The last decade has been a time of rapid change in policing. Major forces have been buffeting police departments for some time. On one hand, the economic crisis has shrunk police budgets and forced police executives to reevaluate all of their operations and even their fundamental missions. At the same time, police departments across the nation and abroad are developing many new technologies that have the potential to make policing more efficient and effective. Social media can be counted as one of these important new technologies.

Because of all the changes going on in the field, it is an interesting and challenging time to be a police leader. PERF and the COPS Office see our roles as helping law enforcement executives share information with each other about what they are learning as they work through the new issues they are encountering. This report is part of that effort. We hope you will find it interesting and informative.

Bernard K. Melekian, Director
Office of Community Oriented Policing Services
U.S. Department of Justice

Chuck Wexler, Executive Director
Police Executive Research Forum

Acknowledgments

PERF would like to thank the U.S. Justice Department's Office of Community Oriented Policing Services (COPS Office) for providing the opportunity to research and explore the emerging issue of social media in policing. Many observers have noted that social media is creating fundamental changes in how people communicate with each other and obtain information. These changes are impacting policing just as they are affecting other fields. This report is one of the first to discuss how social media is being used in police tactical operations.

We would like to extend our thanks to COPS Office Director Bernard Melekian for supporting this project. Katherine McQuay and Zoe Mentel of the COPS Office also provided critical assistance throughout this project. We also would like to thank Target Corporation, in particular Mahogany Eller, for their support on this project.

Thanks also go to the police chiefs and other law enforcement executives, academics, and other professionals who participated in the Executive Session on Social Media and Tactical Law Enforcement in October 2011 in Philadelphia (see Appendix A for a list of attendees). We are especially grateful to those who made presentations at the meeting, including Commissioner Chuck Ramsey of the Philadelphia Police Department, Chief Ed Flynn of Milwaukee, Chief Tim Dolan of Minneapolis, Chief Kenton Rainey of the Bay Area Rapid Transit (BART) Police, Philadelphia Mayor Michael Nutter, and Deputy Chief Peter Sloly of the Toronto Police Service.

This publication would not have been possible without the information we received from individuals we interviewed, and from the agencies that hosted us during site visits (see Appendix B). We obtained important information and guidance from Chief Rainey of the BART Police Department, Chief Jim Chu and other representatives of the Vancouver Police Department, Commander Blake Chow of the Los Angeles Police Department, Deputy Chief Constable Gordon Scobbie of the Tayside Police in the U.K., and Detective Superintendent Steve Dower and other representatives of the Metropolitan Police Service in London. And we would like to extend special thanks for our site visit to the New York Police Department, especially to Deputy Commissioner Mike Farrell, Deputy Inspector Dennis Fulton, and all who worked with us. We would also like to thank the Toronto Police Service for hosting a site visit, especially Chief William Blair, Director Mark Pugash, and Deputy Chief Sloly.

Introduction

The 21st century is becoming known as an Age of Technology, and one of the most important and complex types of new technology is social media. At its core, social media is a tool for communication that has become an integral part of daily life for people of all ages. Social media accounts for 22 percent of time spent on the Internet,[1] and even among people age 65 and older—who are not generally considered prime users of new technologies—one in four people are now active on a social media website.[2] Facebook claimed to have 955 million monthly active users worldwide at the end of June 2012.[3]

Law enforcement agencies, like many other types of organizations, are finding ways to use social media to disseminate information to the public. In fact, police agencies in larger cities are finding that their communities *expect* them to have an online presence on platforms such as Twitter, Facebook, and YouTube.

Police departments also have begun to explore the use of social media to obtain information, especially for tactical purposes, such as gathering information about threats of mob violence, riots, or isolated criminal activity during otherwise-lawful mass demonstrations.

Social media has now given protesters the ability to informally and very quickly organize and communicate with each other in real time. Police must know how to monitor these types of communications in order to gauge the mood of a crowd, assess whether threats of criminal activity are developing, and stay apprised of any plans by large groups of people to move to other locations.

Similarly, in the aftermath of an incident of mob violence, police can "mine" social networking sites to identify victims, witnesses, and perpetrators. Witnesses to crime—and even perpetrators—often post photographs, videos, and other information about an incident that can be used as investigative leads or evidence.

Police agencies must also consider how their own actions are reported to the public through social media. Nearly any action taken in public by a police officer may be recorded on a mobile device and instantly uploaded to YouTube or another social networking site. Many of today's police chiefs have said that they generally advise their officers to always behave in public as if they are being recorded, because that very well may be the case.

Another consideration is that crime victims and witnesses can quickly transmit information about a crime scene or criminal act out to the world, impeding a detective's ability to control the release of information about a case.

The strategic challenges of monitoring social networks and transforming huge amounts of data into actionable intelligence can be a daunting task for police agencies. As one official described it, "It is like trying to take a sip from a fire hydrant."

1. See http://blog.nielsen.com/nielsenwire/global/social-media-accounts-for-22-percent-of-time-online/.
2. See www.cbsnews.com/stories/2010/11/15/national/main7055992.shtml.
3. See http://newsroom.fb.com/content/default.aspx?NewsAreaId=22.

The use of social media in policing is an issue that has only begun to emerge in the last few years, so policy appears to be lagging behind practice to some extent. In a recent survey of 800 law enforcement agencies in the United States, 88 percent of agencies reported using social media, yet only 49 percent had a social media policy.[4] Some police leaders have said they find the process of developing policies helpful in improving their understanding of the issues surrounding social media.

Project Background

This publication is part of a series of reports on emerging issues that are being examined by the Police Executive Research Forum (PERF) with support from the Office of Community Oriented Policing Services (COPS Office). The goal of this project is to examine social media in policing from two tactical points of view:

1. The use of social media by criminal offenders to organize or facilitate criminal events
2. The use of social media by law enforcement agencies to manage large gatherings of people, investigate crimes, or handle other events

(With the exception of Chapter 1, this report does not focus on the use of social media by police departments to disseminate information to the public. Many police chiefs would argue that that is a more important function for social media than the tactical purposes of gathering information. But it is a subject that is receiving a good deal of attention in other reports.)

Our research on social media and tactical law enforcement considerations included site visits at police agencies and interviews with law enforcement leaders in the United States, Canada, and the United Kingdom. In addition, on October 13, 2011, PERF hosted an Executive Session in Philadelphia, which brought together approximately 50 law enforcement leaders, government officials, scholars, and subject matter experts to discuss their experiences with social media for tactical purposes.

Chapter 1 of this report describes the experience of the Toronto Police Service as it developed a social media policy. Chapter 2 identifies intelligence considerations, including the various types of social media monitoring used by two units in the New York City Police Department. Chapter 3 outlines strategies to address robberies and other violent crime committed by flash mobs, as seen in three cities: Philadelphia, Minneapolis, and Milwaukee. Chapter 4 identifies the roles of social media during riots and violent social disturbances in the United Kingdom and Vancouver. Finally, Chapter 5 describes the social media aspects of organized demonstrations and freedom of speech issues experienced by the Bay Area Regional Transit Police Department in 2011.

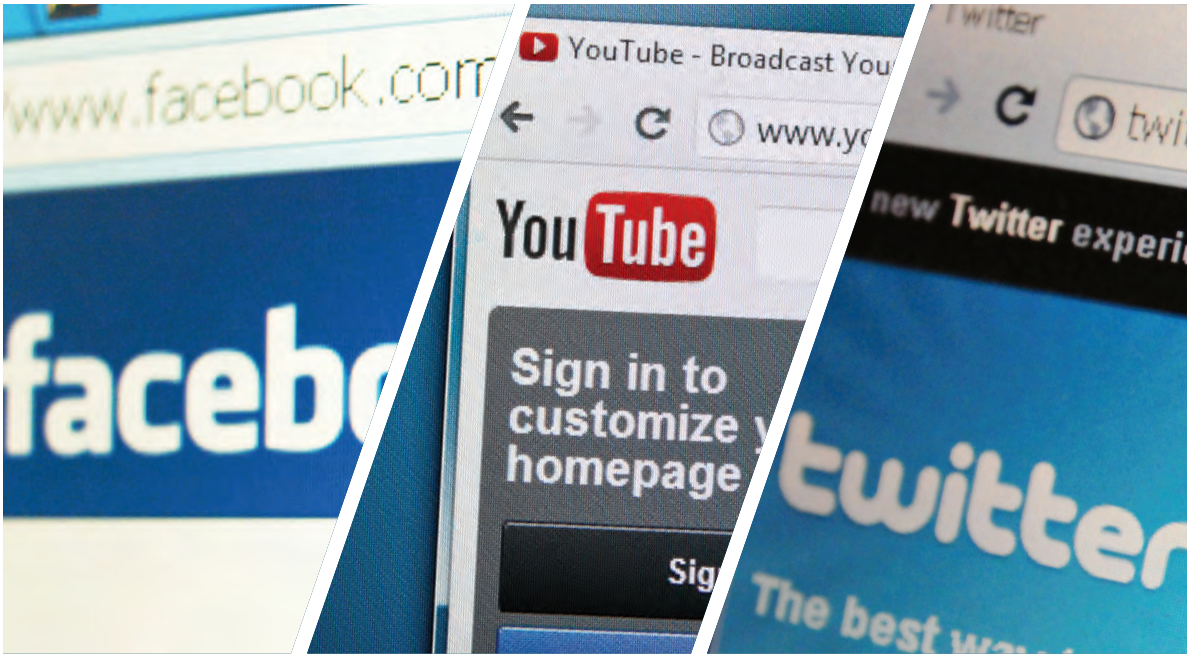
4. See www.iacpsocialmedia.org/Resources/Publications/2011SurveyResults.aspx.

CHAPTER ONE:
Developing a Strategy on Social Media

Many police departments have begun to use social media in tentative or experimental ways. But because the social media phenomenon is relatively new, many police agencies have not yet taken a more comprehensive approach to considering their overall philosophy and approach toward social networking.

The Toronto Police Service (TPS) has a reputation in the field as one of the most advanced law enforcement agencies in the use of social media. *There are currently over 200 individuals in the TPS who have received training and are authorized to use social media to communicate on behalf of the department.*[5]

Following is an account of TPS's early initiatives with social media, dating as far back as 2007, as well as TPS's development of a comprehensive social media strategy in 2010–2011.



One Agency's Experience: The Toronto Police Service

Social media and communications technology companies have become an important part of the Toronto-area economy in recent years, to the extent that there has been some discussion of whether Toronto should aim to become a "Silicon Valley of the North." So it was no surprise to many members of the Toronto Police Service when residents began to have extended communications on social networking sites about public safety issues. A few young police officers and supervisors recognized the need for TPS to participate in certain online conversations, particularly with regard to crime prevention and traffic issues, and they didn't want the agency to miss a potentially valuable opportunity.

5. Readers are encouraged to view the TPS Social Media page at www.torontopolice.on.ca/socialmedia/ for links to the Twitter, Facebook, and YouTube pages of many TPS employees across the department.

"Early Adopters" of Social Media within the Police Service

Constable Scott Mills, an officer in TPS's Public Information Unit, was one of the first officers to bring social media to the attention of his supervisors. Constable Mills was involved in the Toronto Crime Stoppers program, a 25-year-old organization of concerned citizen volunteers who solicit information and tips on crime from the community. Crime Stoppers uses traditional media outlets such as posters, television public service announcements, billboards, and newspaper features to gather information. In 2007, Constable Mills began to feel that TPS was "missing the boat" on social media. According to Chief William Blair, Mills understood that many of the people whom Crime Stoppers wanted to reach didn't watch the local six o'clock news or read newspapers. Instead, young people with information about crime in the community were getting and sharing news and information via social media platforms and other Internet-based sources.

Constable Mills posted the first Crime Stoppers video on YouTube in April 2007, launching a new way for Crime Stoppers to connect with the public. Chief Blair admitted to having some reservations about using YouTube, but he agreed to the initial posting, and the public response was overwhelmingly positive. The number of tips coming in to TPS increased exponentially.[6] Following the YouTube campaign, Toronto Crime Stoppers created a Facebook page and a Twitter account.

Sergeant Tim Burrows, an officer in TPS's Traffic Unit, saw how successful social media was with Toronto Crime Stoppers, and began using it in the Traffic Unit in 2009. Burrows noticed that Toronto residents were using social media to post their "pet peeves" and other information about traffic-related issues. Burrows began to actively participate in the discussions, using Twitter, Facebook, and YouTube to reach out to the community, offer information, answer questions, and discuss traffic and road safety issues.

Developing a Comprehensive Strategy

By 2010, TPS Deputy Chief Peter Sloly was noticing the early efforts at bringing social media to the Police Service, and he recognized that there was a need for a larger, more structured approach. He attended the first international "SMILE" conference (Social Media, the Internet, and Law Enforcement), held in Washington, D.C., in April of that year.

Taking a devil's advocate approach, Deputy Chief Sloly brought a group of officers to the conference who he believed would be able to identify risks or potential problems with using social media in a police agency. But after attending the conference, he said, the officers saw the potential benefits and did *not* try to convince him or TPS Chief William Blair to step back from social media.

Sloly obtained Chief Blair's approval to undertake a comprehensive project to develop a TPS "corporate strategy." As the director of the project, Sloly organized a working group of TPS officers as well as a contractor with expertise in social media in a law enforcement environment, LAwS Communications, which was the organization that held the SMILE conference.

Sloly, the working group, and the contractor then developed a strategy for achieving wide-ranging goals for social media within TPS. These included creating policies to ensure "sound governance" in the ways in which TPS officers post information or otherwise use social media, developing a training module for officers who are chosen to engage in social media, finding ways to use social media to improve communications *within* TPS as well as communications to the public, and creating a plan to measure whether social media efforts are effective.

6. "How Constable Scott Mills's social media work protects Toronto." Digital Journal, Sept. 16, 2010. http://digitaljournal.com/article/297670.

These efforts culminated in the official launch of TPS's social media program on July 27, 2011. That day, the first class of TPS employees who had completed a newly developed social media training course was given authorization to represent the department via social media. Since that time, scores of additional officers have completed the training and have launched Twitter or Facebook accounts to communicate about issues in their sphere of influence.

Chief Blair and Deputy Chief Sloly have discussed a number of general guiding principles for social media in policing. They emphasize that while social media is a useful tool for communication, its use must ultimately support TPS's goal of fighting crime. "Social media is not a silver bullet," Sloly said. "It enables us to do old business in newer ways, but we still have to do old business."

And from the beginning, TPS has emphasized two-way communications between officers and the public. Social media should not be just another "megaphone" for the police to spread their messages; it should be used to solicit communications from the public to the police as well, Sloly said.

One important element of the TPS strategy is that in many cases, TPS officers who see a role for social media in their jobs have been allowed to "self-select"—asking to undergo the social media training, and develop their own TPS social media profiles. It is important to note that these are not personal social media accounts, but rather official TPS accounts.

In the early years of social media, TPS's focus was on using social media externally, to communicate with the public. But under the comprehensive strategy, TPS is working to improve internal department communications using social media platforms as well. Social media facilitates communications between members of the department, independent of rank structures and chain of command. For example, Deputy Chief Sloly maintains a visible command-level presence online, directly communicating with officers—commenting on items they post on Facebook, retweeting their Twitter posts, and linking with them on LinkedIn.

As the use of social media for communications increased within the TPS, crime-fighting applications became apparent. Detectives began to look at social networking communications produced by persons of interest in their criminal investigations.

And when large-scale, high-profile events have taken place in Toronto (e.g., the 2010 G20 Summit and Occupy Toronto protests), the agency's experience with social media platforms made it more nimble in reading and understanding protesters' social media communications, in order to identify potential problems or clear up miscommunications between the police and the public.

One social media-related issue that emerged from the 2010 working group discussions was "cyber-vetting" of potential TPS employees—i.e., evaluating job candidates' online presence and reputation. Because police employees must be trustworthy, candidates may be unsuitable if they have posted comments or other content on social media sites that is perceived as damaging to the trust that a police department must earn with the public. For example, obscene, racist, or reckless comments made by a job candidate on Facebook or Twitter can disqualify candidates or raise serious questions about their judgment and character.

A TPS sub-group worked on this issue and produced several pages of policy and guidance on cyber-vetting, based in part on a policy guide published by the International Association of Chiefs of Police (IACP).[7] The TPS policy provides that

7. See www.theiacp.org/PublicationsGuides/ResearchCenter/Publications/tabid/299/Default.aspx?id=1333&v=1.

cyber-vetting may be conducted only by certain designated TPS employees. The purposes of cyber-vetting are to verify information provided by the candidate at other stages of the application process, to identify candidates who have posted material that indicates involvement in or association with criminal activity or individuals, and to identify candidates whose online behavior goes against TPS's core values. The policy provides that candidates should not be asked for their passwords to social media sites, and cyber searches will not unlawfully bypass candidates' privacy settings on social media sites.

Ensuring Quality Control in Social Media

TPS's Corporate Communications unit helps to guide the scores of TPS personnel who communicate on behalf of the agency via social media platforms. For example, the Corporate Communications unit has issued a one-page guide with basic tips, including the following:

- **"Your accounts are yours but they represent us.** You are free to comment and speak on matters that you have an expertise or working knowledge of, but you are not official spokespersons of the Service…"
- **"The Internet is forever.** Search engines, screen capturing,…and other technologies make it virtually impossible to take something back. Be sure of what you mean to say, and say what you mean."
- **"Be sensitive to the privacy of others and the Service**. Do not share any information of others including their photos without their permission…."
- **"Treat others as you want to be treated.** Always be respectful and patient with others."[8]

The Corporate Communications unit informally monitors communications on TPS social media accounts in order to ensure that TPS officers are maintaining high standards of quality and are adhering to the Service's guidelines.

The Corporate Communications unit also keeps an eye on what members of the public are saying about the Police Service. Only publicly available communications are observed. With the exception of several low-cost or free programs (e.g., Radian6 or TweetDeck), no specialized equipment is used for this monitoring. Typically, the comments and conversations that concern TPS are about high-profile criminal cases and incidents involving the police.

Communications are sometimes reviewed to gauge the public mood, particularly following specific incidents that may lead to anti-police sentiment. According to Director of Corporate Communications Mark Pugash, if a TPS employee makes an inappropriate statement or commits some other error, it is important to monitor the public reaction in order to ensure that TPS can respond quickly and directly. It can be effective to respond in the online forums where an incident is already being discussed, rather in other venues that may not reach the persons who are most concerned about an incident. In some cases, there may be false or misleading statements about the TPS that online responses can help to correct.

TPS also has expanded its analysis of social media during large events and mass demonstrations. During the 2010 G8 and G20 Summits in Toronto, TPS used two officers on 12-hour shifts to analyze public opinion and communications by protesters. A review of keywords and hash-tags showed that the citizens more frequently used Twitter as they sought information about road closures, mass transit disruptions, and police and demonstrator movements. Those posting negative comments about the police used Facebook more frequently than other social media platforms.

8. See www.torontopolice.on.ca/publications/files/social_media_guidelines.pdf.

At one point, TPS had to shut down the ability of people to post comments on TPS's main Facebook wall, because the Service was unable to keep up with the large quantity of posts. Like many police agencies, TPS posts "Terms of Use" for its Facebook pages, stating that TPS may remove viewer comments that are racist, defamatory, threatening, obscene, or otherwise "inappropriate or offensive."[9]

(Managing viewer comments on a police department Facebook page can be a difficult issue. The Honolulu Police Department changed its Facebook posting policy to an open-posting rule after litigants claimed in a federal lawsuit that the department deleted posts that were unfavorable to the department.[10])

During the 2011 Occupy Toronto protests, on several occasions TPS responded to false online allegations that the police were storming the Occupy camp or taking other action against the group. Social media was used to reassure and educate the public.

Because social media is used extensively by organizers and participants in major protests and other large events, TPS is exploring the possibility of having a social media commander at such events, whose presence in the command center would allow the police to respond more quickly to changing developments.

Training

TPS conducts two distinct training sessions that cover issues related to social media. The first is a three-day course about the use of social media by members of the Toronto Police Service to communicate with and engage the public. The second course is a comprehensive five-day training session offered to investigators regarding a variety of computer-facilitated crimes, investigative strategies, and use of social media in criminal investigations.

Training Course on Communicating with the Public: The first training course, developed as part of TPS's 2011 social media strategy, is conducted by personnel from the Corporate Communications unit. The course is believed to be unique among Canadian police agencies, and TPS has received requests from other agencies seeking to send representatives to the training. (As of this writing, limits on resources have prevented TPS from making the course available to other agencies.)

Selection of TPS employees for the course is based on a unit commander's careful assessment of whether an individual is a good candidate to serve as a public voice of the TPS. This is based partly on the candidate's understanding of the concepts of risk management and professionalism. As in other types of organizations, there are certain members of police departments who lack the perspective and judgment to speak on behalf of TPS in such a highly visible way.

The Corporate Communications staff also realized early on that if a police employee lacks enthusiasm about social media or lacks a strong desire to engage people online, that employee should not be given a role in social media. Such an employee would consider social media duties just another task to perform, and would quickly grow weary of it.

9. The complete Terms of Use are available at: www.facebook.com/TorontoPolice?sk=app_250633484947250.
10. "HPD allows unrestricted posting on its Facebook page." *Honolulu Star Advertiser*. September 6, 2012. www.staradvertiser.com/news/breaking/168869326.html.

The first day of class provides an introduction to the TPS social media project, so trainees will understand the considerations made by the agency as it established its social media policy and training. Social media and professional standards are discussed in the context of the overall corporate communications plan for TPS. Participants are given examples of how to effectively communicate to the public through original outgoing messaging, by leveraging other online information sources, and through responses to incoming messages from the public.

The second and third days of training are held in a computer lab, and participants create user accounts that are compliant with TPS standards. Users are provided with basic tutorials on the two most commonly used social media sites, Facebook and Twitter. A good portion of one day is spent learning about Facebook security settings. Participants are also provided with electronic versions of TPS logos, disclosure statements, and other guidance to promote uniformity of appearance in all TPS-sponsored accounts.

At the end of the course, each of the newly created accounts is registered with the TPS Corporate Communications office. Sergeant Tim Burrows provides informal mentoring to each of the individuals trained in the program and routinely checks in with them online. Other TPS members, including agency leaders with an online presence, also provide informal monitoring through their online interactions. Members' accounts are also periodically reviewed to determine whether they are being kept up to date and that the authorized user is using social media well. If there are weaknesses, TPS Corporate Communications tries to determine whether the person needs more mentoring or training. In some cases, a person who starts enthusiastically finds that social media is not his forte. A formalized review process with specific evaluation benchmarks is in development.

Training Course on Computer-Facilitated Crime and Investigative Strategies: An experienced cybercrime detective leads a five-day training course in computer-facilitated crime for investigators. The course is designed for division-level detectives, but not for persons involved in covert or undercover assignments. The course topics include:

- Internet investigations, including IP addresses and tracing websites
- Social media searches and source intelligence
- Facebook account management, privacy settings, and data searches
- Cellular telephones and devices, Internet service providers, and cell tower data
- Search and seizure of computers, cell phones, and related devices
- Forensic analysis of computers, cell phones, and related devices
- Cross-border investigations, multi-agency cooperation, and other law enforcement resources
- eLearning tools and resources for continuing education

Strategies and Lessons Learned

- **Do not allow an over-sensitivity to risk assessment to derail the process of developing social media.** There will always be individuals in any organization who focus on the potential pitfalls of a new technology or process. Police leaders should focus on the potential rewards of using social media and then work to mitigate risks.
- **Keep your policy clear and the language simple.** As with the creation of other types of policy, it was vital to TPS to involve all relevant stakeholders in the creation of its social media strategy. Model policies are helpful starting points, but TPS stressed that customization is important. Policy-makers should ensure that use of social media complies with local, state/territory, and federal laws, as well as with the user agreements of the social media providers.
- **Identify the right people to use social media.** Police agencies should carefully consider whom they want to empower to take visible public roles for the organization. Not everyone is a "natural" at speaking and writing clearly, with sensitivity to political and social issues and other considerations. However, training can help many people improve their skills in this area. If you choose the right people, they will view social media as an integral part of their position, not as a time-consuming add-on to existing duties.

Although most people with an interest in taking a social media role will already be familiar with the basics of Facebook, Twitter, and other media, be prepared to train your people on the context of their use. Talk with your officers to see what they may already be doing with social media and ask how they might do it better with agency support. Make sure that official use of social media by police employees is consistent with the police department's overall communications strategy.

- **Determine the desired visibility level for the agency's chief executive.** Toronto Chief William Blair recognizes the significant role that social media plays in the day-to-day policing of Toronto. However, in an effort not to dilute his own messages as police chief, Chief Blair avoids communicating via social media on a frequent basis. The chief has found it useful to periodically participate in an informative YouTube video or interview, but generally saves his comments for issues of the greatest importance. Thus, if the chief personally conducts a press conference or provides statements on an issue, it is a signal to the public that the TPS considers the issue especially important.
- **Determine whether your policy must cover potential misuse of social media.** Early on, the TPS decided that it did not need to address issues of misconduct in its social media policy. Misconduct, including disclosure of confidential information and failing to represent the department in a professional manner, is already covered in other policies. Problems may occur less often than you expect, Deputy Chief Peter Sloly indicated. "Our people are more professional and better communicators than we tend to give them credit for," he said. He also pointed out that misconduct committed via social media can be easier to investigate than other types of misconduct, because social media postings are recorded. There is automatically a record of the act of misconduct or potential misconduct, making investigations more clear-cut.

- **Determine where you want to begin with your strategy.** If your department is new to social media, it may make sense to begin a social media program internally. Teach your personnel to use their social networking skills internally and then advance to external communications and a community-focused program. Bringing in a social media expert as a consultant may help to give the program credibility in the eyes of your officers and the public.
- **Decide who will be in charge of social media in your agency.** Some departments may develop social media in the divisions or units with the most direct and visible community interactions (e.g., patrol, crime prevention, traffic, and school resource officers). Others may restrict official postings in social media to members of the public information and communications unit. TPS warned against placing a social media coordinator within every unit or patrol division, saying that instead, there should be one central communications strategy, to include social media communications, for the entire department.
- **See the full potential of social media across the police department.** Social media should not be seen merely as a tool for improved "corporate communications," in the view of Toronto Deputy Chief Sloly. "Rather, social media should be mainstreamed into all operations, from crime prevention to intelligence gathering, from next-generation computer-aided dispatch to criminal investigations, public order management, and community policing," he said. "It also must become one of the main Information Technology tools for reducing costs and improving public values in areas like human resources, professional standards/risk management, finance and administration, information management, performance management, and public/private partnerships. As of 2012, the Toronto Police has social media applications in all these areas. Social media and digital platforms are transforming the private/public sectors of society. Police leaders can and must embrace social media and use it to help transform policing in order to keep pace with society."

CHAPTER TWO:
Investigative and Intelligence Considerations

With the rapid expansion in the use of social networking by law-abiding citizens as well as criminals, many law enforcement agencies are feeling the need to have a team of experts to study social media activity. The intelligence developed through effective observation of social media communications can have a significant impact on tactical police operations.

Police departments across the country have noticed that users of Facebook and other social media often make comments and post photographs and videos that incriminate themselves or other people. For example, gang members often post photographs of themselves illegally holding firearms. In some cases, persons have "bragged" about committing serious violent crimes, apparently believing (incorrectly) that police do not look at social media postings or that they are unable to act on information that is posted online.

To ensure that a police department's social media experts can produce high-quality, actionable intelligence, agencies must consider a number of issues, including: which types of online content should be viewed, who will conduct the observation and analysis, and how information will be communicated to operational commanders and field officers.

Few Court Precedents Yet

The legal aspects of social media in investigations have not yet been tested in court to a great extent. One key issue is whether information posted on social media sites such as Facebook is constitutionally protected as private under the Fourth Amendment. Another unresolved issue is whether it is constitutionally permissible for police to set up fictitious identities in Facebook accounts or other social media in order to obtain photos, videos, and other content posted by other Facebook users.

In one case filed on August 10, 2012, the U.S. District Court for the Southern District of New York held that the government did not violate the Fourth Amendment when it accessed information from a suspect's Facebook profile that the suspect classified as "private" under the Facebook privacy settings he chose for his Facebook account.[11] The government obtained the information with the assistance of a cooperating witness who had been "friended" by the suspect, and who thus had access to the potentially incriminating information, which included messages about past acts of violence and threats of new acts of violence against rival gang members.

"[The suspect's] legitimate expectation of privacy ended when he disseminated posts to his 'friends' because those 'friends' were free to use the information however they wanted—including sharing it with the Government," the court said.[12]

11. *U.S.* v. *Joshua Meregildo et al.,* 11 Cr. 576 (WHP), August 10, 2012. www.x1discovery.com/download/US_v_Meregildo.pdf.

12. Ibid.

Police Use of Social Media for Investigations Is Widespread

Law enforcement agencies across the country apparently are moving to use social media in investigations, which could provide greater opportunities for test cases in the courts. **According to a July 2012 survey by LexisNexis Risk Solutions, of 1,221 federal, state, and local law enforcement agencies that use social media in some way, four out of five agencies said they use social media for investigations.**[13]

In fact, viewing posts on social media for criminal investigations was the most common use of social media by the responding agencies.

Other purposes were reported by fewer agencies, such as conducting background investigations of job candidates (cited by 31 percent of agencies that use social media); "community outreach to build public relations," 26 percent; notifying the public of crimes, 23 percent; and notifying the public of traffic issues, 14 percent. More than 80 percent of the responding officials said they believe that social media will be "critically important in the future" for crime fighting and investigative purposes, that "creating personas or profiles on social media outlets for use in law enforcement activities is ethical," and that "social media is a valuable tool in investigating crimes." And 48 percent of responding officials said they already use social media in investigations at least two to three times per week.

Respondents in the LexisNexis survey offered examples of how they use social media in investigations, including the following:

Evidence Collection: "It is amazing that people still 'brag' about their actions on social media sites,…even their criminal actions. Last week we had an assault wherein the victim was struck with brass knuckles. The suspect denied involvement in a face-to-face interview, but his Facebook page had his claim of hurting a kid and believe it or not, that he dumped the [brass knuckles] in a trash can at a park. A little footwork…led to the brass knuckles being located and [a confession] during a follow-up interview."

Location of suspects: "I was looking for a suspect related to drug charges for over a month. When I looked him up on Facebook and requested him as a friend from a fictitious profile, he accepted. He kept 'checking in' everywhere he went, so I was able to track him down very easily."

Criminal Network Identification: "Social media is a valuable tool because you are able to see the activities of a target in his comfortable stage. Targets brag and post…information in reference to travel, hobbies, places visited, appointments, circle of friends, family members, relationships, actions, etc."

Our study focuses on the use of social media for investigative and intelligence purposes by the New York City Police Department (NYPD). As the largest police department in the United States, the NYPD has resources not available in many smaller agencies. However, the lessons learned by the NYPD in studying social media communications have implications for agencies of all sizes.

13. LexisNexis Risk Solutions, 2012. *Survey of Law Enforcement Personnel and Their Use of Social Media in Investigations.* www.lexisnexis.com/investigations.

One Agency's Story: The NYPD

Like most big-city police departments, the NYPD uses social media such as Twitter and Facebook to share information with the public about crime patterns and crime prevention tips, major events in the city, the response to disasters such as Hurricane Sandy, and other matters. As of November 2012, the NYPD's Twitter account, @NYPDnews, had more than 47,000 followers, and more than 86,000 people had clicked the button indicating that they "like" the NYPD's Facebook page, www.facebook.com/NYPD.

Like most large departments, the NYPD has officers in a number of different units who analyze social media for crime-fighting purposes. In a recent review of its officers' social networking use, the NYPD found that 72 percent of its social networking use was by the detective bureau. However, units with other roles (e.g., intelligence, counterterrorism, gang enforcement, internal affairs, and executive staff identity protection and threat assessment) have begun to develop social media programs, and these units have begun to request better tools to facilitate their work.

Although much of the NYPD's analysis of social media postings is done through basic open-source search engines, the NYPD is considering the possibility of using a number of commercially available business software tools.

Two of the units working most actively to analyze social media are located in the NYPD's Intelligence Division and the Juvenile Justice Division. Within the Intelligence Division, a specialized group of officers has been tasked with watching social media for communications regarding large-scale events and criminal activity. The Intelligence Division also assists other units with criminal investigations. The Juvenile Justice Division focuses on analyzing social networking by local youth gangs and neighborhood crews.

Although their work is very different, these two units mine similar online sources for intelligence. Facebook, Twitter, and YouTube produce the largest amount of information for these units. To a lesser extent, listservs and other social media sites are also observed.

Any use of social media by an undercover officer to actively engage individuals is extremely rare in these two units, and is carefully reviewed by the department as part of a set of guidelines that regulate NYPD monitoring of political activities.[14]

In September 2012 the NYPD issued a formal operations order governing the use of social networks for investigative purposes. The order's provisions include the following:

Use of aliases: When members of the Police Department require access to a social network website for investigative or research purposes and need to create an online alias, they must confer with their supervisors, who document the requests and submit them to the commanding officer for review. The documentation includes information about the purpose of the request, the user name to be used as an alias, and the photograph to be used with the alias, if any. Records must be kept about these requests. Thus, the order ensures that NYPD management will be monitoring the use of aliases in investigations involving social media.

14. The Handschu Agreement dates to a 1971 class-action case against the NYPD and requires that any investigation by the NYPD involving political activity, including investigations on social networks, must be initiated by and conducted only under the supervision of the Intelligence Division.

Public domain data: No authorization is required for online searches of information that is in the public domain. That is defined as "information accessible through the Internet for which no password, e-mail address, or other identifier is necessary to acquire access to view or collect such information." (For example, some users of Facebook adjust their privacy settings so that only persons whom they have accepted as Facebook friends can view what they post, while other users choose to make photographs, comments, or other information that they post online available to the general public.)

Suspected terrorist activity: If an application for an online alias involves suspected terrorist activity, the supervisor must immediately contact the NYPD Intelligence Division, which will decide whether the investigation should be conducted by the Intelligence Division.

The importance of social media in investigations by the Intelligence and Juvenile Justice Divisions has been demonstrated repeatedly. Crimes as serious as homicide and shooting at police officers have been solved with publicly posted YouTube videos and Facebook page comments. In addition, potential violence at "jump-up" parties and mass demonstrations has been averted as police were able to mobilize in advance of the events.

Following are more detailed descriptions of the social media work by these two divisions:

Intelligence Division

A specialized unit within the Intelligence Division has been tasked with monitoring social networks, 1) for advance warning of events that could require a police response, and 2) for criminal investigations. Led by Deputy Inspector Steven D'Ullise, the unit has a mix of experienced detectives and younger officers. D'Ullise explained that this mix helps to ensure that the unit has knowledge of current technologies and street jargon, which tend to be the expertise of young officers, while also having the requisite institutional knowledge and investigative experience.

Cases and assignments generally reach the unit by one of two methods:

First, a precinct detective squad or field intelligence officer may contact the unit and request that it begin viewing the online activities of a particular person or group for the purposes of a specific investigation. Online activity for these cases is compiled for evidentiary purposes or to identify crime victims, witnesses, and perpetrators.

One recent example occurred following the firing of shots at officers from a high-rise apartment complex. Soon after the incident, a YouTube video was posted online that led officers to a previously unidentified witness. The video also helped to identify the location from which the shots were fired.

In the case of a homicide or other serious or high-profile crime, the social media unit may initiate social media reviews and searches even before being approached by assigned investigators. This is important because often, perpetrators of crimes or others with knowledge of a crime may delete postings from social media sites within hours of an incident.

The second type of case assignment in the social media unit involves proactively preventing illegal activities. For example, "bus parties" and "jump up parties" in New York City have at times resulted in violence and criminal activity. When the social media unit learns of a party—typically through an online flyer or Facebook posting—detectives can contact limousine companies or event venues to make them aware of the nature of the party, and give them the opportunity to cancel their involvement if they are concerned about the likelihood of criminal activity. In the case of large parties at private homes or at abandoned buildings or other illegal locations, officers may be able to break up the parties before they begin. If the police have little advance warning of an illegal party, they still may be able to shut it down before it becomes a large-scale event.

Within constitutional limits, the social media unit also studies information about mass demonstrations and protests. Social media postings can provide information about the date, time, and location of a protest, or about the events of a particular day during an ongoing event. Postings also can provide minute-by-minute information about the size and demeanor of crowds of protesters. Intelligence officers are on the ground before and during events in order to get street-level corroboration of what is being communicated to demonstrators and the public online.

During any large event, the Intelligence Division social media unit is actively viewing live feeds and providing information to the operations center. In very large events, the fusion center may be opened, and trained individuals can be pulled from other intelligence units to analyze online traffic. Commanding officers on the street are kept informed of intelligence developments through their smartphones, and some also follow selected websites and Twitter feeds themselves.

Juvenile Justice Division

In early 2012, a new unit was formed within the NYPD Juvenile Justice Division for the purpose of using social networking and intelligence to combat violent crime perpetrated by youthful offenders, most of whom belong to local neighborhood gangs or crews. A major goal of the unit is to provide useable information to patrol officers and detectives anywhere in the city.

Building upon techniques first used in 2006 to map crews in Manhattan, the unit has begun to map out crew territories block by block for every precinct in New York City. According to the unit's commanding officer, Assistant Commissioner Kevin O'Connor, the unit has been successful because "beefs" between gang members are often communicated on Facebook. In the first three months of its existence, the unit identified and mapped 250 crews, and they expect that number to exceed 300.

Interestingly, Assistant Commissioner O'Connor and his unit make no attempt to hide the fact that they are viewing online postings by crew members. They inform the youths and the general community that they are online. However, youths continue to post information. Ninety-five percent of the youths in crews are said to use Facebook, and a much smaller percentage use Twitter for communications. YouTube has been invaluable for identifying crews and their identities, affiliations, and activities.

Because a great deal of information is passed between crew members online, social network posts have proved helpful to probation and parole officers as well. Using the information from the Juvenile Justice Division's social media unit, officers on the street can better identify who is likely to be involved in a retaliation shooting and where it may occur. In some cases, prosecutors have obtained conditions of probation or parole that prohibit individuals from engaging in online social networking communications with other crew members.

Training Officers on Social Media

Many police agencies provide little, if any, training to their officers on social media. In the NYPD recruit academy and leadership training, the curriculum is focused mainly on police use of social media to disseminate information to the public, rather than on obtaining information for investigations.

Most of the training in the NYPD's specialized social media units is conducted on the job, and is based on the work already being done within the department and the unit. In the Intelligence Division unit, for example, each of the detectives was trained using the same PowerPoint presentation, and they routinely seek knowledge and assistance on cases from one of the detectives who has a computer science background. Deputy Inspector D'Ulisse periodically runs tabletop exercises for the group on new developments and techniques.

Many of today's patrol officers are from a generation that grew up using the Internet. Most routinely use personal social media accounts and are familiar with the nuances of the various platforms. However, in the NYPD's view, that does not mean that patrol officers should shift their focus from their duties on the street and spend time viewing social media postings by potential suspects.

In the NYPD's view, what patrol officers should be trained to understand is that social media units and other resources are available to them. "We don't want patrol officers doing this," said Assistant Commissioner O'Connor. "We want to make sure we can get them the information in a simple, useable format." Patrol officers also should be trained to understand the restrictions that apply to any searches of social media they might conduct.

Summary

As the largest police department in the United States, the NYPD has resources not available in many smaller agencies. However, the lessons learned by the NYPD in analyzing social media communications have implications for agencies of all sizes.

Two social media units, in the NYPD's Intelligence Division and Juvenile Justice Division, review social media postings for several purposes, including investigating crimes, tracking gangs and "beefs" between rival gang members, gathering information about large-scale demonstrations or other events that may require a police presence, and learning about illegal gatherings of people for "jump-up" parties at abandoned buildings and similar events.

Training of officers in the social media units is conducted on the job. The NYPD's approach is that special social media units can provide information to patrol officers or others who need it, and that patrol officers should remain focused on their duties on the street, rather than studying social media on their own. Observing social media legally and responsibly requires specialized technical and legal expertise.

CHAPTER THREE:
Flash Mob Violence and Robberies

Typically a flash mob is a group of individuals brought to one location for the purpose of performing the same act. Sometimes a flash mob is harmless—a group of people gathering at a train station to sing or dance, or to have a friendly snowball fight to celebrate a major snowfall. At other times, a flash mob may commit criminal acts, such as gathering at a store and running out with their arms full of clothing, stolen in plain view, or meeting in a busy entertainment district to fight one another and cause chaos among law-abiding citizens.

For the purposes of this chapter, we will discuss flash mobs that are meant to result in a public disturbance or criminal activity.

One thing that flash mobs tend to have in common is that the participants are familiar with social media and use it on a daily basis. Social media communications (in particular, Twitter, Facebook, and smartphone messaging) are often used to organize flash mobs.

In some cases, individuals with no criminal history find themselves caught up in a "mob mentality" and are tempted to commit vandalism or other crimes they would never commit in other circumstances. Some participants later report that they felt a sense of anonymity in being part of a mob. However, many have learned that there is no longer anonymity in crowds, especially if many people are taking photographs and videos of the event. The photos, videos, and other information are quickly posted on social media, where they can be seen by the police and community members in order to identify lawbreakers.

In some states, legislators are considering stricter penalties for criminal activities like flash mob robberies, in order to account for the larger scale of multiple crimes committed by flash mobs, as opposed to crimes committed by individuals.[15]

Strategies and Lessons Learned From Three Agencies

Police departments have found that there is a good deal of variation in flash mob situations, especially regarding the purpose of the gatherings. In this chapter, we report the experiences of police chiefs and other law enforcement officials in three cities: Philadelphia, Minneapolis, and Milwaukee.

Philadelphia Experiences Several Violent Flash Mobs

Mobs of young people committing acts of violence and other crimes in Philadelphia have been a significant problem in recent years. The groups often use social media applications, such as Facebook and Twitter, to meet in the Center City or other sections of Philadelphia, where they commit thefts or other offenses. Often their crimes are recorded and posted onto YouTube by witnesses or even by members of the flash mob themselves.

15. For example, House Bill 46, introduced in the Maryland Assembly in January 2012, allows for the value of stolen property to be aggregated in determining whether a theft should be considered a felony or misdemeanor, when "multiple acts of theft are committed by multiple individuals…at the same time and in the same place, in concert." http://legiscan.com/gaits/text/513949.

Several incidents occurred in 2010, including a large flash mob in a Macy's store just blocks from City Hall. During that event, approximately 75 to 100 youths congregated inside and outside the store, and some ran through the store, causing damage and knocking down customers. The crowd then ran through the City Center area, with some youths fighting and stopping traffic. Fifteen youths were arrested and prosecuted in a consolidated hearing in juvenile court. All but one of the youths were adjudicated delinquent and committed to various juvenile detention facilities.

Two weeks later, a group of approximately 50 to 75 youths congregated at the Gallery Mall in Philadelphia's Center City. The gathering was organized through a Myspace e-mail blast. Again, some youths ran through the Mall and the streets, fighting, knocking over bystanders, and generally frightening the public. In that incident, 19 persons were arrested. Fifteen were adjudicated in juvenile court, where they either admitted or were adjudicated delinquent on charges of riot and conspiracy. Some were committed to a juvenile facility and others were placed on probation. In addition, four persons were charged in criminal court, where they were placed in a diversion program resulting in community service requirements.

In 2011, there were several additional incidents of flash mobs. A large group of teens from Philadelphia entered a Sears department store in the suburb of Upper Darby and shoplifted sneakers, watches, and other items. In another incident, teens left a neighborhood music festival in North Philadelphia, just north of Center City, and proceeded into Center City, where some of them assaulted people in a business and restaurant district. At least four men were injured, including a 55-year-old man who was beaten into unconsciousness. Four youths were arrested, including an 11-year-old. The person who was considered the "ringleader" was committed to a state secure facility, and the 11-year-old was placed on house arrest and probation.

Police Commissioner Charles Ramsey said the police department was initially caught off guard by the first flash mob incidents. The department later learned that youths had been publicly posting their plans for days before the incidents, but the police department was not routinely viewing social media sites. This quickly changed; the police department currently reviews public postings on Facebook, Twitter, and other social media in order to learn in advance about potentially dangerous incidents.

On August 8, 2011, Mayor Nutter announced a coordinated response to the flash mob and teen violence issue in Philadelphia.[16] Working with the support of community groups, business owners, the Philadelphia Police Department, and the District Attorney's Office, Mayor Nutter signed an executive order that temporarily altered the weekend curfews for minors. A temporary curfew of 9:00 PM was imposed on all minors under the age of 18 in two specific problem areas in Philadelphia: Center City and University City. A first offense could result in a citation and fine of $100 to $300, and parents could also be fined up to $500 for their children's further curfew violations. At the same time that these curfews were imposed, community recreation center hours were extended for youths on weekend nights.

The police department realized that flash mobs were not simply a policing issue. The police needed to work with the young people of the city, through coalitions with the mayor and other government agencies, recreation centers, and community organizations. The police department also worked to open a dialogue with parents, calling on them to help the police enforce the curfews. Community leaders throughout the city participated in an "I Pledge" program, where residents pledged to do what they could to stop mob behavior. Several prominent local DJs were also vocal in their opposition to the flash mobs and criminal behavior.

Early in the process, the business community also was engaged in the police department's flash mob response. Center City District (CCD) is a business improvement organization that works with the police to address crime and quality-of-life issues in Center City. The police worked with CCD's director of crime prevention services to ensure that everyone in the residential and business communities in Center City was aware of the flash mob incidents.

As a result, CCD issued a message to Center City businesses regarding the flash mob incidents, which included these tips:

- All buildings should establish security procedures to enable a quick response by management in the event there is an incident, parade, or spontaneous gathering of large groups of people on the street.
- The Philadelphia Police Department has instituted a number of new strategies to address those types of spontaneous gatherings that may cause harm to others, but they need your help and information to be able to respond to the problem area immediately.

When to call 911:

- If building personnel or tenants become aware of unusually large, unplanned groups gathering nearby.
- If you see a large group of youngsters or others who appear to be moving very quickly or running from or to something.
- If you become aware of any unusual activities such as fights, acts of vandalism, aggression, or other unsafe activity.
- When in doubt, please err on the side of caution and make the call.
- Companies can also consider instituting a response plan that includes temporarily locking the entry doors until the crowd has passed. Such security procedures should not cause any harm or create an unsafe situation for tenants, customers, or employees.

16. See www.phillypolice.com/news/mayor-nutter-announces-flash-mob-response-lowers-weekend-curfew-to-9pm-in-targeted-enforcement-areas.

- If an incident arises that involves the gathering of large groups of people, information will be sent out via Alert Philadelphia as soon as it becomes available. Please notify the Center City District of any large groups gathering (after you've alerted 911), which will enable [us] to send out the appropriate information via Alert Philadelphia.

Following is an example of an alert that was distributed by CCD to its member businesses after the police department provided information it obtained from social media and other sources about a potential flash mob threat:

> **Potential for a Flash Mob**
>
> *On Wednesday, March 16, 2011, the Criminal Intelligence Unit received information that a large group of individuals are planning to meet at Love Park located at 1600 JFK Blvd on Friday, March 18, 2011 at 4:30 p.m. and then proceed to South Street by 7 p.m.*
>
> *These groups have been communicating via the Internet on Facebook promoting the event. The event is being hosted by a number of party promotion groups… Some of these groups have been involved in prior "flash mob" incidents in the city.*

Minneapolis Dance Parties Grow Too Large

In contrast to the situation in Philadelphia, flash mobs in Minneapolis began indoors and were forced out to the streets. The situation involved large dance parties organized in downtown hotels. The parties were advertised as events for young people (some were advertised as "age 16 and under," others as "age 21 and under"). As word of the parties spread via social media sites, text messages, and other promotional activities, the crowds grew to hundreds more than were planned. Security guarantees by the host hotels were misrepresented, and there were a number of situations in which police were called to disperse crowds.

In September 2011 a teen dance party became unruly and approximately 800 young people flooded the Nicollet Mall area of downtown Minneapolis following confrontations with hotel security. Members of the mob began to fight and throw patio furniture outside nearby restaurants. One officer was punched in the face by a partygoer.[17] Video of the event was soon posted on YouTube.

In early 2012, there were several incidents of "click mobbing" where groups of young men in downtown Minneapolis assaulted innocent bystanders. In one case, a group of 15 to 20 youths reportedly attacked three bicyclists and then fled from police.[18] Social media sometimes facilitates the group's planning to meet up in the downtown area, and then the perpetrators pick out their targets for robbery and assaults.

Minneapolis Police Chief Tim Dolan said the police department has responded on several fronts. Prior to any potential event, the department works on prevention. School resource officers are often a valuable source of information about events, as they know many of the youths and hear about potential problematic activities before they occur. The department also monitors social media sites for talk about specific events and parties.

17. See www.kare11.com/news/article/937991/396/Police-arrest-3-after-mini-riot-in-Minneapolis.
18. See www.startribune.com/local/minneapolis/144394085.html.

To prepare for a potential disturbance, members of the police department have studied flash mob incidents in other cities and have been incorporating various scenarios into incident preparedness training. Because the police share a radio channel with private security agencies throughout the downtown area, police are contacted quickly when there are indications of trouble, and they can respond promptly. This radio system also allows the police to alert private security if they obtain information that a large group is moving toward a particular location.

Individuals arrested for participation in these mobs tend to be first-time offenders, and police have found them to be a useful source of intelligence. Debriefing arrestees has helped investigators to identify party organizers, mob instigators, and others involved in violence or criminal activity.

One other strategy utilized by the Minneapolis Police Department is to directly approach problematic venues, including hotels and dance halls, and warn them against holding events that appear likely to get out of control. After one venue ignored requests to cancel an event and the police were called to break up a large, unruly group of young people, the police department billed the hotel for its services. The department's intention is to send a message that organizers of large events must take responsibility for security planning.

Milwaukee Encounters Trouble at State Fair

On the night of Saturday, July 3, 2011, a melee broke out in the Riverwest section of Milwaukee. As crowds left the annual Big Bang Fireworks celebration, crowds on Reservoir Hill, a popular viewing spot, were victimized by a large group of violent people. Victims were beaten and kicked; beer bottles were thrown; and property was taken. Two blocks away, a gas station was looted.[19]

Later that summer, during the August opening of the Wisconsin State Fair, which borders the city of Milwaukee, another rampage resulted in 11 injuries and more than 30 arrests.[20] Fights broke out among a number of young people at the midway, and video was soon posted to YouTube and Facebook. Later that night, violence escalated into additional random assaults.

19. See www.jsonline.com/news/milwaukee/125027704.html.

20. See www.jsonline.com/news/milwaukee/126828998.html.

As the police began their investigation, intelligence officers in the fusion center downloaded videos from YouTube and posts from Facebook and Twitter. They began to immediately monitor postings about the incident and reviewed historical posts. It appeared that, while the State Fair incident had not entirely been pre-planned through social media, members of multiple gangs had been alluding to violence at the state fair via social media for several days in advance.[21]

Police Chief Ed Flynn said the incidents were a catalyst for the police department to think about how they could better monitor social media to avert future violent events. In just one month after the State Fair incident, at least six large potentially violent events were prevented or disrupted by police because they had advance warning and intelligence, developed by analyzing social media.

Strategies and Lessons Learned

Although the levels of violence and other aspects of the incidents described above vary, there are similarities in the police responses and the lessons they have learned. Commissioner Ramsey, Chief Dolan, and Chief Flynn share a concern about the flash mob phenomenon and a desire to use social media in order to stay a step ahead of violent mobs and keep their communities safe.

Below are recommendations from these chiefs and other participants in the PERF Executive Session:

- **Analyze Social Media –** Agencies should actively view Facebook posts, Tweets, and other social media communications to develop actionable intelligence for preventing violent or otherwise illegal flash mob events. In most agencies, officers will "passively connect" with individuals in order to be included in information distribution and see discussions about potential criminal activity.
- **Identify Groups with Histories of Criminal Activity –** Officers should become familiar with various groups that have an online presence, so police will be able to distinguish credible information from rumors. Police also should strive to distinguish large groups from smaller sub-groups that may have criminal intentions. For example, in Milwaukee there are a number of dance crews that organize dance-offs in local parks. Some violent gangs have splintered off from these otherwise lawful dance crews and have created their own presence on social media and in the community.
- **Use Social Media for Outreach –** Police should get to know youths and their parents and should open dialogues with both groups. Many police agencies have successfully used social media to communicate with teens about flash mobs. Following several high-profile flash mob incidents along Michigan Avenue in downtown Chicago, the police department used Twitter to communicate to parent groups, school groups, and youths that the police would not tolerate mob violence and crime.
- **Get the Community Involved –** Flash mob incidents are not only a law enforcement issue. The police should work with local government elected officials, schools, other government agencies, community leaders, recreation centers, faith-based organizations, and other local representatives to address the problem.
  - In Philadelphia, several popular local disc jockeys have been influential in denouncing mob violence and robberies. This can be helpful, because youths will be receptive to messages from celebrities they trust.

21. See www.jsonline.com/news/crime/127630118.html.

- **Curfews** – Curfews have proved useful in some cities under certain circumstances. In the case of the Wisconsin State Fair, leaders were able to impose restrictions on admission of minors after 5:00 PM.
  - In Philadelphia, there have been curfew laws in place since the 1950s, but the laws were not particularly strict. Juveniles from 13 to 17 could stay out during the summer until midnight, and youths under age 12 until 10:00 PM. After the flash mob incidents, the mayor imposed a temporary 9:00 PM curfew in certain neighborhoods. On the first night of that curfew, 40 minors were arrested. On subsequent nights, the number of arrests went down significantly, because people knew that the law was being enforced.
  - After the temporary curfew was lifted, the City Council changed the curfew ordinance. Under the updated law, which the mayor signed on November 14, 2011, minors 13 and under have a curfew of 8:00 PM during the school year and 9:00 PM during the summer. Youths age 14 and 15 have a 9:00 PM curfew during the school year and 10:00 PM during the summer. Youths age 16 and 17 have a 10:00 PM curfew during the school year and 11:00 PM during the summer.
- **Business District Initiatives** – Police departments can work to improve communications with businesses in areas that have been impacted by flash mob robberies and violence. This can be done by providing information to businesses—and obtaining information from them—through meetings and presentations, e-mail blasts, social media, or other methods. In Minneapolis, police have existing partnerships with local business groups that include the use of a radio channel for police and private security officers. This radio system is useful in sharing information about potential flash mob groups or incidents.
- **Prevent Events** – Several police agencies noted that sometimes they can prevent large gatherings that appear likely to result in violence. They speak to the event organizers or the managers of the venue prior to the event. In Minneapolis, large dance parties and gatherings have been misrepresented to local venues as smaller gatherings, and organizers sometimes provide inadequate security for the events. Social media promotion of the event can result in overcrowding and violence.

- **Use Other Intelligence Resources –** School resource officers are frequently a good source of information about youths' activities. They should be trained to understand flash mob events and alert other police units when they learn about a potentially dangerous event. Debriefing arrestees, particularly first-time offenders, can result in a wealth of information that can identify organizers, participants, and groups' strategies.
- **Transit Enforcement** – In urban areas, flash mob participants often use mass transportation to travel to areas where violence occurs. When police have information about a potentially violent flash mob event, they may be able to prevent youths from traveling to the site. For example, in Chicago and New York, police found that many of the teens were jumping subway turnstiles on the way to flash mob events. By enforcing fare evasion statutes, police prevented individuals from reaching those locations.

CHAPTER FOUR:
Using Social Media to Prevent, Respond to, and Investigate Riots

Another area in which police departments can benefit from experience with social media is the handling of riots. Participants and bystanders often use social media to discuss the possibility of rioting in advance of an event, and they use social media during an incident to share information about what is happening. Police can obtain information about possible threats or other intelligence by paying attention to social media posts by members of the public. Police also can use social media to disseminate information to the public during an incident, to detect any false information that may be circulating, and to correct the erroneous information. In addition, police can use social media following a riot for investigative purposes.

This chapter presents two case studies to explore issues of social media in the context of violent social unrest:

- **Vancouver Canucks incident:** In June 2011, the loss of a hockey championship triggered several hours of rioting in Vancouver, BC.
- **U.K. riots over Mark Duggan shooting:** In August 2011, several days of rioting occurred in London and other cities following the fatal shooting by police of a 29-year-old man named Mark Duggan.

This chapter presents the two case studies in three sections:

1. Use of Social Media during the Riots
2. Use of Social Media in the Post-Riot Investigations
3. Use of Social Media for Community Outreach After the Riots

Use of Social Media during the Riots

Vancouver Canucks Riot

On June 15, 2011, the Vancouver Canucks lost the final game of the National Hockey League championship to the Boston Bruins. Before and during the game, an estimated 155,000 fans came into downtown Vancouver. Many fans watched the game on giant televisions at viewing areas downtown.

Immediately prior to the final playoff game, there was some speculation on social media and in the mainstream media of a potential riot. However, no credible intelligence emerged that suggested a riot would take place. Some of the speculative posts were from people who did not reside in Vancouver. Moreover, the Vancouver Police Department (VPD) has encountered several instances in which people attempted to use social media to organize and coordinate civil disobedience—without such behavior taking place.

However, when the Canucks lost, separate riots began almost simultaneously at two different flashpoints in the downtown core and lasted just over three hours, overwhelming the police resources on the ground. At the beginning of the evening there were about 500 police and Traffic Authority officers deployed, and this number swelled to over 900 officers by the night's end. Approximately 140 people were treated at two downtown hospitals. While many of the reported injuries were related to tear gas exposure, the casualties also included at least eight stabbings as well as cases of major trauma, head injuries, fractured ankles and legs, a broken jaw, and a collapsed lung.[22]

22. New York Times, June 16, 2011. "Trouble in Vancouver's Streets After Defeat." www.nytimes.com/2011/06/16/sports/vancouver-fans-take-to-the-streets-after-loss.html.

The VPD had anticipated that there might be unrest if the Canucks lost the hockey game, and had established a tactical plan to counteract a possible riot. However, the massive and incredibly dense crowd, the large number of rioters, and the fact that the rioting was occurring at different locations simultaneously, quickly exceeded the capacity of the resources.

The Stanley Cup play-offs were the first time the VPD used Twitter at a large event and where the Social Media Officer worked inside the VPD Operations Centre. During the play-off games, the Social Media Officer used Twitter to communicate information to the public regarding safety issues, traffic routing, and crowd control. Throughout this time, the Social Media Officer also used Hootsuite to monitor keywords referring to any civil unrest, and although there was chatter on Twitter around the word "riot," establishing the credibility or validity of tweets was problematic. Hundreds of tweets flooded into the @ VancouverPD Twitter account after Game 7, and the Social Media Officer answered many questions and concerns from citizens while continuing to tweet transit information, safety updates, and reassurances to the public.

Within 20 minutes of the riots starting, tweets with potential suspect information or photos were received, but there was no procedure in place to gather this information or to advise people what to do with their photos. Tweets were sent by @VancouverPD advising witnesses to hold onto their footage until a protocol for receiving this information could be established in the days following.

As the rioting continued, the VPD used social media as a tool to get instructions to the public and mitigate any misinformation being broadcast to the community though traditional media (e.g., television and radio coverage) and social media. Almost 3,000 new people started following the VPD's Twitter feed during Game 7 and the subsequent riot, with the total number of followers increasing from 10,400 followers at the start of the game to 13,170 by midnight. The following days saw an additional 2,000 followers.

A subsequent investigation of the riot determined that social media did not play a role in the organization of rioters. The vast majority of rioters who confessed to their involvement admitted they came downtown to watch the game and because of their high level of intoxication got "caught up in the moment." This "celebratory" sports riot was spontaneous and fuelled by instigators who were cheered on by large crowds. The typical Vancouver rioters were young people, mostly without a criminal record and from middle-class backgrounds, who did not reside in the city.

The main role of social media was reflected in the recording devices that were in the hands of the thousands of onlookers. Five thousand hours of video and thousands of digital images were recorded by onlookers, and many digital files were posted on social media during and after the riot—some by the rioters themselves. This digital evidence became crucial to the success of the massive criminal investigation to follow.

U.K. Riots after Mark Duggan Shooting

On August 4, 2011, Mark Duggan was fatally shot by an officer of the Metropolitan Police Service (MPS) in the Tottenham area of North London. The circumstances were unclear on several points, and an organized protest was held on August 6 to protest the actions of the police.[23] Although the protest began peacefully, it escalated into rioting, possibly triggered by criminals who were not involved in the vigil, according to an MPS spokesman.[24]

23. See www.guardian.co.uk/uk/2011/aug/06/tottenham-riots-protesters-police.

24. See www.guardian.co.uk/uk/blog/2011/aug/07/tottenham-riots-police-duggan-live#block-44.

Over the next few days, news about the disturbances in Tottenham sparked looting and mass violence in the London districts of Brixton, Enfield, Islington, Wood Green, and in Oxford Circus, as well as many smaller towns and cities in England.[25] Although the disturbances in Tottenham were initially blamed on strained relations between the police and the black community in that area, the causes of the disturbances in other areas have been subject to extensive debate.[26]

During the disturbances, MPS's tactical response was led by commanders at the Operation Center. A representative from the Met Intelligence Bureau (MIB) was present to help determine what events had occurred, to predict what could happen next, and to determine what else the Operations Center needed to know in order to ensure the safety of the public and the police officers. The MIB worked to collect information from social media and more traditional sources.

However, the speed of unfolding events required a level of organization that was not possible. More than 4,500 people were arrested in connection with the riots in multiple locations. Officers in the MIB had not been formally trained in gathering information from social media, and they did not know how to organize and synthesize this information once it was gathered. The MIB found that it was overwhelmed by the amount of incoming data; it was difficult to sort good from bad information, much less turn it into actionable intelligence. In some cases, poorly organized, unsynthesized, and sometimes false or extraneous information was turned over to commanders, leaving them unsure how to use the information in their tactical plans.

According to the Detective Superintendent Steve Dower of the MIB, it quickly became apparent that social media amplifies the amount of information available to the police. In order to capture and monitor the massive amounts of information available through social media, the MIB needed to refocus its efforts. The unit has begun to increase its preparedness through training on social media sources, evidence collection, and recognizing actionable intelligence. Another point of discussion was whether to centralize intelligence functions in a unit that would focus on the on-going impact of social media.

Lessons Learned

Although the London riots were different from the Vancouver riot, officials from both police departments reported learning similar lessons based on the following principles:

- **It is important to have pre-established channels of social media communication.** In Vancouver, the police department already had established itself on social media and had been actively working with the public to communicate information and have a dialogue with the community. While MPS had a Twitter page, it was being used only in a limited capacity to make formal announcements. MPS had no informal means of mass communication to quickly get information out to the public. Since the 2011 Duggan riots, MPS has recognized that social media is the best way to reach certain segments of the population, and social media operations are being worked into future strategies and tactical planning.
- **Agencies should use experienced intelligence officers to determine the value of social media information and tips.** In both Vancouver and the U.K., a large amount of information was transmitted to the police, and there was tremendous difficulty in sifting false information from the accurate information prior to and during the riots.

25. See www.bbc.co.uk/news/uk-10321233.

26. See www.bbc.co.uk/news/uk-14436529.

- **Agencies must work to get accurate information out to the public.** In Vancouver, rioters and members of the public seemingly ignored VPD's posts and tweets while responding to inaccurate information posted by others. For example, members of the media posted on Twitter that Vancouver's SkyTrain stations, a way for the public to leave the downtown area, had been closed. That was not the case, but many people remained downtown, believing that they were stranded. It was helpful to have the Social Media Officer working inside the VPD Operations Center alongside a member of the Transit Police so that accurate transit information could be tweeted. To combat the problem of inaccurate information being disseminated, in the future VPD will examine technology to allow police to directly broadcast official information to cell phones in the immediate geographic area of an incident.


Photo: Nic Neufeld/Shutterstock.com

Use of Social Media in the Post-Riot Investigations

Vancouver Canucks Riot

As stated above, a massive amount of digital photography and video recording took place during the riot in Vancouver. Investigators were faced with processing over 5,000 hours of raw video in more than 100 formats. By comparison, there were approximately 100 hours of videotape available at another hockey riot in Vancouver in 1994. Throughout the course of the three-hour riot in 2011, which resulted in scores of injuries, looting, property destruction, arsons, and assaults, thousands of onlookers and participants recorded criminal actions on their mobile devices.

In fact, the 2011 Vancouver riot has been called the world's first "smartphone riot," because of the ubiquity of these devices and the fact that many people, instead of running from the carnage, remained in the area to watch and record it. Perhaps some rioters were motivated to commit their acts of violence and vandalism because they were performing for the cameras—without realizing that the people for whom they were performing were also gathering evidence of their crimes. After the riot, many of these thousands of hours of videos and thousands of still images were posted on YouTube, Facebook, and Flickr.

To investigate this massive incident, the Vancouver Integrated Riot Investigation Team (IRIT) was formed, led by the VPD and composed of 70 investigators and analysts from the VPD, other municipal police agencies, and the Royal Canadian Mounted Police. IRIT set up an e-mail account where people could send tips or videos, so all the information would be in one place. In the first week, IRIT received more than 3,500 tips from the community. IRIT also issued a public appeal for recorded images of the riot. This was accomplished through a series of planned press conferences that leveraged the high public interest in seeking out the identity of the rioters. During the early stages of the investigation, the VPD appealed to the public not to engage in online vigilantism, but rather to send their evidence to the police. There were some unfortunate cases of innocent people being "outed" on social media. In addition, many others, including juvenile offenders (who cannot be identified publicly by police by law), were visibly shamed on social media sites.

Once images of rioters were isolated by IRIT investigators, a dedicated website was established to allow the public to review photos and to provide names and contact information for suspects whom they recognized. The website has been successful as an investigative tool in identifying persons who participated in the riots. According to Chief Constable Chu, the interactivity of the website allowed the public to identify perpetrators, and placed pressure on offenders to turn themselves in.

In order to spread the word about the dedicated website, IRIT used traditional communication methods, including press conferences, as well as Twitter. VPD tweets were used to direct the public to the IRIT riot website. Despite the availability of digital communications channels, IRIT also produced two "Riot Roundup" posters, which were handed out by volunteers throughout the Vancouver region. Each poster displayed 104 rioters, and 40,000 copies of the first poster and 70,000 copies of the second were produced. These "wanted" posters generated news coverage, which in turn further promoted the IRIT website. The posters were displayed at schools, which also produced new tips and additional visits to the IRIT website.

One particularly violent attack was directed at a Good Samaritan who tried to stop the looting of a department store and was attacked by 15 assailants. IRIT investigators identified 14 out of 15 suspects with help from the public. A further appeal was made to the news media to identify this 15th suspect. Two tips came in that reported this person to be a resident of Winnipeg who had been in Vancouver as a temporary construction worker. The suspect was arrested and charged.

As of October 2012, IRIT has recommended for prosecution 872 charges against 275 persons. VPD expects the final number of accused persons to be over 300.

U.K. Riots after Mark Duggan Shooting

In the United Kingdom, digital images were collected from social media and closed-circuit TV cameras directly after the disturbances. The public was generally eager to help identify those who were involved. The Metropolitan Police Service (MPS) also used anonymous tip lines and other traditional forms of collecting information from the public.

During the riots, many of the looters did not bother to cover their faces as they raided and destroyed shops. Some posed for pictures with stolen goods, posting them on social networking sites.

In general, MPS used a three-part method in gathering evidence. First, they used Facebook and other social media sites to gather information and intelligence, synthesizing it into usable evidence. Second, they used traditional methods such as anonymous tip lines and digital forensics to collect information directly from mobile phones and other handheld devices. Finally, through lawful acquisition of communications data, officers were able to recover more evidence. This was particularly important in the case of evidence that had been deleted from users' pages and sites.

MPS was able to gather enough evidence to make more than 4,500 arrests, of which more than 2,900 have resulted in prosecutions, and nearly 1,300 people have been sentenced to prison terms, averaging 17 months.[27]

27. See http://sports.yahoo.com/news/police-monitor-vigil-riots-death-man-113022193.html.

Lessons Learned

MPS and VPD quickly realized that their investigations and evidence collection process would be challenged by the vast amount of data pouring into their agencies in the days after riots. Following are some of the lessons they learned:

- **Explore innovative ways to collect information and tips from the public.** Previously, MPS tended to use traditional ways to collect information and appeal to the public for assistance, such as anonymous tip lines and seizing smartphones and other handheld devices in order to directly download photos, videos, and other information from them.
  - Although these methods were successful, an anonymous "Catch a Looter" blog that was *not* associated with the police service was instrumental in publishing images of looters and allowing people to submit information online.[28] The blog, which posted images of looters, was an innovative way for the public to become involved, as well as an easy way to submit vital information needed to further police investigations.[29]
  - In Vancouver, a Facebook ad campaign was developed to specifically target the demographic best able to assist investigators. Over 160,000 15- to 27-year-olds received ads on their Facebook profiles that would link them to the VPD riot website.
- **It is important to have working relationships with social media providers.** MPS had a working relationship with social media companies regarding lawful acquisition of communications data. This saved time during the riots following the Duggan shooting. Police knew whom to contact in the social media companies and what to expect in terms of their response.
- **Make public appeals for information immediately after the incident.** It is important not to delay in asking the public for assistance and providing the details about how people should provide information. Response may be greatest while people are still reacting to the immediate impact of the incident, before public interest wanes. This was achieved by developing a coordinated media strategy and dedicating an experienced media officer to monitor and assess opportunities for public appeals and messaging.
- **Ensure that your agency has the capacity to handle a large flow of incoming information.** Agencies need to have mechanisms in place before an incident occurs, so that information can be collected instantly, rather than a few days after the occurrence. The VPD requested that the public send tips to an e-mail account created for this purpose, and the amount of information received was overwhelming. It took many weeks to review all the information provided to the VPD, but the police had the information in hand because their system for collecting it worked.

28. See www.huffingtonpost.co.uk/tara-harrison/diy-justice-catch-a-loote_b_922088.html.

29. Ibid.

- **Take care to fully investigate all relevant tips and information.** It is important to be somewhat skeptical of all tips and social media data. After the riots in Vancouver, there were concerns about whether images posted online and sent to the police might be "photoshopped" or otherwise altered to show false information.
  - Even when videos or photos were not tampered with, there was concern about whether they might be misleading. For example, a video might not include important aspects of an event that occurred in the minutes before or after the video was recorded. And still photographs may have been taken from an angle or with a type of lens that distorts the actual appearance of the subject, inadvertently or intentionally. For example, wide-angle lenses tend to exaggerate the distance between the camera and the subject and the distances between different subjects in a photograph, while long telephoto lenses tend to "compress" distances and make it appear that subjects are closer together than they are.
  - One example of misleading information involved a man named Brock Anton, who was identified as one of the first instigators of the Vancouver riot.[30] He bragged online about punching police officers, turning cars upside-down, and committing other crimes. However, after analyzing videos of Anton throughout the incident, VPD learned that he was boasting about crimes that he did not commit. Needless to say, he was not charged with those offenses.
- **Do not abandon traditional techniques.** In order to aid the investigation of the Canucks riot, the VPD released a "digital wanted poster" website of suspects who had not yet been identified. This provided an outlet for the public to provide information that was different from other sites about the riot, which were sometimes slanted toward vigilantism.

  While the VPD had success with its "digital wanted poster" website, it also used more traditional methods to distribute images of suspects to the public. Officers distributed posters to the public at bus and train stations, busy downtown intersections, and other high-pedestrian locations. More than 100,000 posters were handed out by hundreds of volunteers, blanketing 19 cities across the region. This generated a high level of interest from the news media and played a significant role in involving the public in the investigation. Following the poster campaign, investigators received leads on over half of the riot photos depicted in the posters.

  Social media should enhance these traditional techniques, not replace them.
- **Be alert to vigilantism.** There also was a negative use of social media after the riots: to organize vigilante campaigns. In Vancouver, a Facebook group called "Vancouver Riot Pics: Post Your Photos" posted hundreds of pictures of suspected rioters to be identified by the public. The most well-known identification made on this website was of a young Canadian from the junior Olympics water-polo team, who was photographed attempting to set a police car on fire. The young man promptly apologized, but he was suspended from his water polo team. Vigilantes posted his home address online, and his family moved into hiding after receiving threats.[31]

30. See http://voices.yahoo.com/brock-anton-face-vancouver-riot-8672631.html.

31. See www.huffingtonpost.ca/bill-mann/vancouver-riot-social-media_b_889017.html.

— In the United Kingdom, a teenager named Dane Williamson was falsely accused and charged with setting fire to a store during the Manchester disturbances. After these initial charges were brought, his name and addressed were spread across the Internet. While Williamson was being held in prison, vigilantes set his apartment in Salford on fire, in retaliation for the fire he supposedly set during the disturbances. A short time later, he was cleared of all charges and released from prison to find he had lost all his possessions and was now homeless.[32]

— In both Vancouver and the U.K., police issued statements urging the public to reject vigilante behavior.

Use of Social Media for Community Outreach after the Riots

There was a third aspect to the use of social media following the riots in Vancouver and the United Kingdom: The communities used social media to help in the clean-up of the damage caused by mobs and looters. Volunteers came together to clean up downtown Vancouver the morning after the riots, and throughout London and other parts of the United Kingdom, similar recovery efforts were undertaken.

Vancouver

VPD tweets and Facebook were used to inform the public of upcoming communications and press conferences. Chief Constable Chu also streamed a "virtual town hall meeting" over the Internet called "Tweet the Chief." It had a reach of more than a quarter million people. The VPD now has more than 26,000 Twitter followers.[33]

VPD also used social media to directly connect with local businesses affected by the riots. VPD contacted several Business Improvement Associations in the riot-affected areas and sent e-mails over their networks to provide information about the investigations.

London

The MPS is focusing on using social media to foster community engagement. Previously, MPS's communications unit was the only one using social media to communicate with the public, and the official Twitter page for MPS was merely announcing official information, rather than engaging the public. Units such as the Met Intelligence Bureau were missing out on opportunities to build online relationships with segments of the population.

MPS is currently working with other law enforcement agencies in the United Kingdom to create standards and consistency in social media use. The goal is to ultimately have all 43 law enforcement agencies in the U.K. using best practices in developing social media.

Lessons Learned

- **Use social media to inform the community about how to provide constructive assistance.** Such efforts not only help to repair the physical damage to communities, but also create a spirit of goodwill while fostering communications between the police and residents.

32. See www.guardian.co.uk/uk/2011/aug/21/dane-williamson-cleared-manchester-riots.

33. See http://vancouver.openfile.ca/blog/curator-blog/explainer/2011/police-chief-hang-twitterverse.

CHAPTER FIVE:
Mass Demonstrations: The Law Sometimes Lags behind Advances in Technology

When faced with civil disobedience or mass demonstrations, police departments must maintain public safety while also protecting individuals' right to freedom of speech. Police strategies for managing large demonstrations have evolved in recent years, generally in the direction of making greater efforts to engage demonstrators and assure them that the police recognize law enforcement's role in protecting First Amendment rights. Law enforcement leaders also have developed best practices for preventing unnecessary uses of force and minimizing the arrests of demonstrators.[34]

With the development of new communications technologies, including cellular telephones, text messaging, and social networking, the ways in which groups prepare, organize, and congregate has changed. Protesters often use Twitter and text messages to make their plans and to share information about the progress of a demonstration, about police responses at various locations, and about other aspects of an event.

Police agencies' responsibilities for protecting citizens' First Amendment rights have become more complex, as new ways of communicating have been invented and have become commonplace.

A textbook example of this phenomenon took place in San Francisco in 2011, when the Bay Area Rapid Transit (BART) Police Department was faced with demonstrations following the police shooting of a homeless man on a subway platform. **At issue was whether police may shut down cellular telephone service in order to prevent protesters from engaging in potentially illegal and dangerous actions inside the subway system.**

As of September 2012, the legal issues remain unresolved. But experts believe that the courts eventually will play a role in defining whether law enforcement agencies can limit the public's use of social media during demonstrations.

This chapter describes the issues raised by the BART case.

Bart Police Department

Can Police Use Prior Restraint to Limit Communications during a Demonstration?

On July 3, 2011, a 45-year-old homeless man named Charles Hill was fatally shot by a Bay Area Rapid Transit police officer at San Francisco's Civic Center transit station. BART said that police responded after receiving a call about "a drunk man who was unsteady on his feet and in danger of falling off the platform," and that investigators believe that when officers arrived at the scene, "the suspect used a bottle and a knife as weapons and behaved aggressively."[35]

34. A summary of these strategies is available in Managing Major Events: Best Practices from the Field. Police Executive Research Forum, 2011, www.policeforum.org/dotAsset/1491727.pdf.

35. "Investigators working to identify suspect killed in BART officer involved shooting." BART news release, July 5, 2011, www.bart.gov/news/articles/2011/news20110705a.aspx.

At the time of the Hill shooting, BART police were facing substantial criticism for the 2009 fatal shooting of Oscar Grant III. A month earlier, former BART police officer Johannes Mehserle had been released on parole after being convicted of involuntary manslaughter in shooting Oscar Grant. Mehserle's defense attorney had argued that the officer intended to use his Electronic Control Weapon against Grant but mistakenly used his firearm.

On July 11, demonstrators gathered at the BART station where Hill had been killed to protest the shooting. According to a statement later issued by BART, during the July 11 protest, "one person climbed on top of a train and many other individuals blocked train doorways and held train doors open. During the course of the event, which occurred during the peak of rush hour, individuals…caused the shutdown or partial shutdown of other stations. These actions violated the law by creating a serious threat to the safe operation of the BART system, disrupting the service of 96 BART trains,…causing the closing of stations, and putting at risk the safety of thousands of passengers and BART employees."[36]

Plans for a Second Protest

BART said that about a month after the Hill shooting, it received credible information about additional protests to be held at certain BART station platforms on August 11. This information included reports of plans for "lawless activity on the platforms," as well as indications that the August 11 protest could be much larger than the July protest, BART said.[37]

Intelligence received by the BART Police as of August 10 "revealed that the individuals would be giving and receiving instructions to coordinate their activities via cell phone after their arrival on the train platforms at more than one station," BART said.[38] "Individuals were instructed to text the location of police officers so that the organizers would be aware of officer locations and response times."

As a result, BART said it concluded that "the planned action constituted a serious and imminent threat to the safety of BART passengers and personnel and the safe operation of the BART system." Based on that assessment, BART decided to interrupt cell phone service at targeted portions of its system for up to 4 hours, beginning at 4:00 PM, the time that the individuals were scheduled to assemble. The goal was to prevent a potentially dangerous massing of protesters on train platforms. BART notified the cellular service providers shortly before it implemented the temporary interruption. Service was turned back on at 7:00 PM, earlier than planned, when safety concerns abated, BART said.

Civil Liberties Advocates See Attempt to "Silence Critics"

The lack of cell phone service apparently had the effect of thwarting any plans for a demonstration and lawless activity, because the planned protests did not materialize.

Civil liberties organizations and other observers expressed outrage at the shutdown of cellular service in the BART system. The ACLU of Northern California sent a letter to BART Chief of Police Kenton Rainey calling the action a violation of the First Amendment guarantee of free speech, and demanding that BART promise not to take similar actions in the future.

36. "A letter from BART to our customers." August 20, 2011 news release from BART President Bob Franklin and Interim General Manager Sherwood Wakeman, www.bart.gov/news/articles/2011/news20110820.aspx.

37. Ibid.

38. Ibid.

"All over the world, people are using mobile devices to protest oppressive regimes, and governments are shutting down cell phone towers and the Internet to silence them," ACLU Executive Director Abdi Soltani and Legal Director Alan Schlosser wrote.[39] "BART has never disrupted wireless service before, and chose to take this unprecedented measure for the first time last week in response to a protest of BART police. BART's decision was in effect an effort by a governmental entity to silence its critics."

Cell Phone Access an Unresolved Legal Issue

U.S. Supreme Court precedents on the First Amendment guarantee of free speech provide a number of exceptions in which certain types of speech are given limited protection or no protection under the First Amendment. These include exceptions for obscenity and child pornography, libel and slander, commercial speech, and speech on radio or television.[40]

One famous exception to the First Amendment guarantee of free speech, established by the Supreme Court in 1919, is speech that creates "a clear and present danger" to public safety, such as "falsely shouting fire in a theater and causing a panic."[41]

Under a 1969 case that further defines that exception, the First Amendment provides no protection to speech that constitutes "advocacy of the use of force or of law violation…where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action."[42]

It was that public safety exception that BART had in mind in explaining its reasons for shutting down cellular service in an attempt to prevent protesters from engaging in lawless activity and taking over subway platforms. "When trains are not able to move or pick up passengers, the platforms can quickly become overcrowded," BART's open letter to the public said. "This is very dangerous due to the increased possibility that people will fall from the platforms onto the trackway. The trackway is five feet below the platform edge and contains the electrified 3rd rail. Also, when one train stops, all trains behind it must stop. In some cases, trains must stop in tunnels, which delays the arrival of emergency medical help for passengers in need of assistance. Additionally, self-evacuation by passengers in underground tunnels is another potential dangerous outcome of interference with BART service."[43]

The ACLU rejected that explanation, saying that "speech does not lose its protection merely because it may lead indirectly to disruption."

Furthermore, shutting down cellular service constitutes "prior restraint," rather than the less restrictive alternative of allowing speech to be made and then filing a criminal prosecution or civil suit as a legal remedy for any violation of law, the ACLU noted. Supreme Court precedents have established an especially heavy presumption against prior restraint of speech.

39. ACLU of Northern California letter to Kenton W. Rainey, August 15, 2011, https://www.aclunc.org/issues/technology/blog/asset_upload_file335_10381.pdf.
40. *Freedom of Speech and Press: Exceptions to the First Amendment.* Congressional Research Service. 2009, www.fas.org/sgp/crs/misc/95-815.pdf.
41. *Schenck* v. *United States*, 249 U.S. 47, 52.
42. *Brandenburg* v. *Ohio*, 395 U.S. 444, 447.
43. "A letter from BART to our customers." August 20, 2011 news release, www.bart.gov/news/articles/2011/news20110820.aspx.

"There can be no question that shutting down wireless service is an unconstitutional prior restraint," the ACLU letter to Police Chief Rainey said.[44] "Such a move would be tantamount to prohibiting the printing and dissemination of all newspapers because of concerns that a single letter to the editor may include plans for a protest."

New Issue: Is a Suspension of Cell Service a Free Speech Violation?

Legal experts noted that BART did not literally stop protesters from speaking, but rather ordered the *shutdown of cellular service* that protesters might have used to communicate with each other. Whether a shutdown of a cell phone system can be a First Amendment violation is an issue that is too new to have been settled by the courts.

In an interview with National Public Radio, UCLA Law Professor Eugene Volokh noted that BART was merely limiting cell phone service in certain areas of its own property, and that those areas—on the platforms and in the tunnels—are not areas that would be considered a public forum from a legal standpoint. He added that public universities sometimes block wireless access in their buildings for a much less serious reason than public safety: to reduce disruptions in classes by students using their phones.[45]

The ACLU had a different perspective that courts might find compelling, however. "BART apparently justifies its position on the ground that there is no free speech on a BART platform," the ACLU letter to Chief Rainey argued. "If BART has its way, that will certainly be the case,…but that does not make it lawful. While the government has no obligation to build a public park, once it does so, it cannot shut the park gates to speakers with whom it disagrees."

Gene Policinski, executive director of the First Amendment Center at Vanderbilt University, suggested that existing free-speech precedents will inform the court decisions that will eventually emerge regarding shutdowns of cell phone service and other First Amendment issues in the Internet age, but it is difficult to predict the outcomes.

"We're not going to throw out 220 years' worth of thinking about the way we communicate with each other, the way we express ourselves, the way we petition government for change, the way we assemble," Policinski said. "So while the technology is a new wrinkle, I think we can look to a lot of settled law and principles that we hold dear to guide us through this. [The BART protest] is the first time this has occurred in this fashion in the United States, and in a way, this debate is going to help us structure how the law moves on from here. I think you'd want to look at a couple of things. First of all, is this prior restraint?…Is there an overriding government interest, which BART is saying is public safety? And then there's the issue of whether a BART platform, a train platform, is a public forum or not. So you've got a lot of First Amendment issues being raised here. It's a very complicated thing from what seems to be at first a very simple issue."[46]

44. ACLU of Northern California letter to Kenton W. Rainey, August 15, 2011, https://www.aclunc.org/issues/technology/blog/asset_upload_file335_10381.pdf.
45. "Cell Service Shutdown Raises Free Speech Questions." *National Public Radio*. August 16, 2011, www.npr.org/2011/08/16/139656641/cell-service-shutdown-raises-free-speech-questions.
46. First Amendment Center experts discuss BART, free speech on radio shows. August 22, 2011, www.firstamendmentcenter.org/fac-experts-discuss-bart-free-speech-on-radio-shows.

BART Develops a Policy on Cellular Disruptions

BART's shutdown of cellular service in certain parts of it system for several hours on August 11 resulted in a good deal of controversy for many months afterward. On August 14, the group known as Anonymous reportedly hacked into and defaced BART's consumer website and released the personal information of 2,400 of the website's 55,000 users.[47] And a number of organizations compared the action to those of repressive foreign governments. The Electronic Frontier Foundation (EFF) released a statement saying, "One thing is clear, whether it's BART or the cell phone carriers that were responsible for the shut-off, cutting off cell phone service in response to a planned protest is a shameful attack on free speech."[48]

The BART Police Department began to work on a formal policy governing such situations, in collaboration with consultants from the Federal Communications Commission, the ACLU, the Citizen's Review Board, as well as the BART Board of Directors and General Counsel. In December 2011, the one-page policy was adopted by the BART board on a 7-0 vote.

The policy states:

> *[BART recognizes that cellular service] should be interrupted only in the most extraordinary circumstances that threaten the safety of … passengers, employees and other members of public, the destruction of [BART] property, or the substantial disruption of public transit service. …[BART] is also fully committed to its existing long-standing policy of allowing the exercise of First Amendment rights of expression in the areas of its stations where it can be done safely and without interference with [BART's] primary mission. …*
>
> *In accordance with these principles, it shall be the policy [that BART] may implement a temporary interruption of operation of the System Cellular Equipment only when it determines that there is strong evidence of imminent unlawful activity that threatens the safety of passengers, employees and other members of the public, the destruction of [BART] property, or the substantial disruption of public transit services; that the interruption will substantially reduce the likelihood of such unlawful activity; that such interruption is essential to protect the safety of passengers, employees and other members of the public, to protect [BART] property or to avoid substantial disruption of public transit services; and that such interruption is narrowly tailored to those areas and time periods necessary to protect against the unlawful activity. ….*
>
> *Illustrative examples of "extraordinary circumstances" include, but are not limited to, strong evidence of use of cell phones (i) as instrumentalities in explosives; (ii) to facilitate violent criminal activity or endanger [BART] passengers, employees or other members of the public, such as hostage situations; (iii) to facilitate specific plans or attempts to destroy [BART] property or substantially disrupt public transit services.*[49]

47. "Anonymous Hackers Attack BART Website." *Mashable Tech*, August 15, 2011, http://mashable.com/2011/08/15/bart-anonymous-attack/.
48. "BART Pulls a Mubarak in San Francisco." *Electronic Frontier Foundation*. August 12, 2011, https://www.eff.org/deeplinks/2011/08/bart-pulls-mubarak-san-francisco.
49. Cell Service Interruption Policy, www.bart.gov/docs/final_CSIP.pdf.

California Legislature Adopts Statewide Restrictions on Shutting Down Cell Service, But Governor Vetoes the Bill, Citing Public Safety Concerns

Civil liberties organizations expressed support for many of the provisions in the BART policy, but noted that the decision to shut down cellular service would still reside with BART.

In August 2012, the California legislature voted to take authority for those decisions, approving legislation that prohibits the suspension of cellular service by public agencies without a court order.[50]

"For decades, California law has required a court order to interrupt or shut down traditional telephone service," said Senator Alex Padilla, sponsor of the legislation.[51] "SB 1160 would extend these protections to the modern telecommunication networks and prohibit the interruption of service by local governments without court review."

However, on September 29, 2012, Gov. Jerry Brown vetoed the legislation. In his veto statement, Governor Brown noted that the bill would require police to apply for a court order within six hours of interrupting cellular service, even in "barricade, hostage and emergency circumstances."

Applying for a court order would require police to make certain legal findings and determinations about the situation, and "the extent of the findings in the bill that must be made by officers engaged in conflict could divert attention away from resolving the conflict without further threat to public safety," Brown wrote.[52]

The governor expressed support for the concept of authorizing interruptions of cellular service "only in the most extreme cases," and urged Senator Padilla and police agencies to develop a new version of the bill "that balances protection of speech with the ability of law enforcement to utilize this tool [interrupting cellular service] in the protection of public health and safety."

50. Legislators back ban on phone blackout. August 13, 2012. *San Francisco Chronicle*, www.sfgate.com/bayarea/article/Legislators-back-ban-on-phone-blackout-3785688.php.

51. Bill to Protect Public's 1st Amendment Rights and Ensure Access to 911 Services Passed by State Assembly. News release by Sen. Padilla, http://dist20.casen.govoffice.com/index.asp?Type=B_PR&SEC={5EACFA15-EA6B-41D8-9711-C030F9FAD5EE}&DE={DAB6BE4C-9E5C-4801-8408-7529F6E0CAB9}.

52. Governor's memorandum to the Members of the California State Senate re Senate Bill 1160, Sept. 29, 2012, http://gov.ca.gov/docs/SB_1160_Veto_Message.pdf.

Conclusion

Following are some of the key findings and recommendations offered by police officials who contributed to this report:

Developing a Social Media Strategy for Disseminating Information to the Public

Do not be afraid to take calculated risks: An oversensitivity to risk assessment can thwart efforts to launch a social media program. It is easy to identify possible problems that could result from using social media, but police leaders in Toronto found that in practice, many of those problems did not materialize. They recommend focusing on the potential rewards of using social media, and working to mitigate the risks.

Identify the right people to use social media: Not everyone is a "natural" at writing clearly and showing sensitivity to political and social considerations. But training can help improve these skills for many people. The people who are best at using social media view it as a useful and integral part of their job, not as a time-consuming chore.

Basic tips to remember: There are certain ideas that always apply to social media, starting with the fact that "the Internet is forever." That is to say, once a statement has been posted online, it can be impossible to take it back. Even if you delete the statement, it may already have been captured or recorded in various ways. So social media users must be careful to say exactly what they mean. Police also must be sensitive to the privacy of others, and should always be respectful and patient.

Look for the implications of social media across the entire police department: The Toronto Police Service and other departments have demonstrated that social media can be used for many purposes, from crime prevention and community policing to intelligence and criminal investigations. It is not merely a function of a police department's public information unit.

Use of Social Media in Investigations and Intelligence Gathering

Be aware of legal issues: Using social media in investigations is not uncommon; in fact, most law enforcement agencies that participated in a 2012 survey said they do so. However, that is not to say that the issues pertaining to this practice have been resolved. To the contrary, the legal aspects of using social media for investigations and intelligence gathering have not yet been tested in court to a significant extent.

Draw a distinction between publicly available information and information obtained by using an alias: The NYPD's written policy governing the use of social networks for investigative purposes makes this simple distinction: No authorization is required for online searches of information that is in the public domain, accessible without any use of a password or other identifier. But if police employees need to create an online alias in order to obtain information, they must request permission from their supervisors, and records must be kept regarding those requests. Thus, the policy ensures that NYPD management will be monitoring the use of social media aliases in investigations.

Consider who will use social media for investigations: Police departments may make different decisions regarding which employees will be authorized to use social media in investigations. The NYPD has decided that it does not want patrol officers to shift their focus from their duties on the street in order to spend time viewing social media postings by potential suspects. But the NYPD believes that patrol officers should be trained to understand what resources are available to them from special units in the NYPD that do conduct such investigations.

Social Media and Flash Mobs

Analyzing social media postings: A number of police departments have experienced incidents in which people use social media to form "flash mobs" to commit thefts or cause disruptions in stores or in certain neighborhoods, to organize large dance parties, or to cause trouble at large public events.

Police departments should become adept at anticipating such activities and at monitoring social media in order to obtain information about the potential for criminal activity. This includes becoming familiar with various groups that have an online presence, so police will be able to distinguish credible information from rumors.

Using social media for outreach: Police can use social media to disseminate information as well as gather information about potential flash mobs and illegal activity. For example, the Chicago Police Department has used Twitter to communicate messages to school groups, parent groups, and youths that the police will not tolerate mob violence.

Other strategies: Police in some cities have developed close working relationships with business district groups and other organizations. These groups can be helpful in providing information to police about potential flash mobs or other incidents, and in spreading information that police wish to disseminate quickly.

In some cases, curfews have helped to prevent illegal activities of the types that can be promoted by social media.

If police see a party or other event being promoted at a venue that appears too small to handle a large crowd, they can contact the owners of the venue to determine if they are aware of the situation and to ask if they have adequate security plans, etc.

Social Media and Riots

Preventing riots: Police departments that have experienced riots fueled in part by social media note that it is important to have pre-established channels of social media communication that were developed before a crisis happens. Police increasingly recognize that social media platforms are the best way to reach certain segments of the population, such as young people who do not watch television news programs or other traditional news media. Information can be exchanged in both directions between the police and members of the public.

Using social media to investigate riots: Due to so many people having become accustomed to using the cameras in their mobile phones, riots or other large events usually are photographed by hundreds or thousands of participants. These recordings often are posted online immediately, or in the days following an incident.

For police departments that want to use such video recordings and photographs to investigate criminal activity, it is important to make public appeals for the information immediately after the incident, before public interest wanes. But police must have the capacity to handle a large flow of incoming information.

Furthermore, police must maintain a certain level of skepticism about such information. Photographs may be "photoshopped" or otherwise altered, for example. Even photos that have not been altered may present a misleading impression, for example, because a wide-angle or telephoto lens may distort the distances between objects in a photo. And a video may exclude events that happened immediately before or after the events depicted in the video, resulting in false impressions.

Police also should be alert to the danger of vigilante campaigns against persons suspected of rioting based on video recordings or other information posted on social media. There have been incidents of persons being falsely accused of crimes and threatened or harmed based on erroneous information.

Social Media and Mass Demonstrations

Use of social media should be part of a comprehensive program of police planning for mass demonstrations and other large-scale events. This issue has been explored in other publications, such as PERF's 2011 report *Managing Major Events: Best Practices from the Field.*[53]

The current report includes discussion of one particular issue that arose in 2011 in San Francisco, when the Bay Area Rapid Transit (BART) Police Department experienced demonstrations after the police shooting of a homeless man on a subway platform. At one demonstration, one person climbed on top of a train and many others blocked train doorways or held train doors open. The BART police said these actions created a serious risk to the safe operation of the transit system, particularly given the tight spaces on train platforms.

BART police later received information about additional protests being planned, including intelligence indicating that protesters would coordinate their activities at particular train stations via cell phone. Believing that the planned demonstrations "constituted a serious and imminent threat to the safety of BART passengers and personnel," BART decided to interrupt cell phone service at certain locations for a period of up to four hours when the demonstrations were planned, in order to prevent the demonstrators from organizing.

Some legal experts noted that subway platforms are not like public parks or other locations that are conducive to mass demonstrations, and thus subway platforms would not be considered public forums from a legal standpoint. However, civil liberties groups argued that the BART action was a violation of the First Amendment guarantee of free speech. Those issues have not yet been resolved in the courts.

In August 2012, the California legislature approved legislation to prohibit the suspension of cellular service by public agencies without a court order. But Gov. Jerry Brown vetoed the bill, citing public safety concerns.

53. Available online at www.policeforum.org/dotAsset/1491727.pdf.

Law enforcement agencies' use of social media is still a new phenomenon. This report touches on some of the issues that have been raised to date about this new medium of communication. In some cases, the issues hinge on legal questions that have not been resolved. And there is no doubt that additional issues will crop up as people find new ways of sharing public safety-related information.

This report is based mostly on the experiences of police departments that are on the leading edge of using social media. In general, these departments are enthusiastic about the potential of social media for improving police operations. They understand the potential for problems, but do not consider the problems a good reason to avoid the technology. The day will never come when all of the issues of social media have been settled. Rather, the technology is constantly changing. In order to understand the social media issues of tomorrow, it will help to have some experience with the issues of today.

In other words, social technology experts urge law enforcement agencies to "get their feet wet" and begin the process of learning how new communications platforms can help them do their jobs. This report is intended to provide guidance from those who have some experience under their belts.

One lesson we have learned is that for police officials, social media is about balancing competing interests. Social media facilitate the sharing of information, and sharing information can help police to protect citizens and prevent crimes. But people are also concerned about their rights to privacy. So police must take care to avoid unnecessary violations of residents' privacy.

Today's police executives do not have a body of court opinions or other rules to guide them as they seek this balance. But common sense and a simple recognition that privacy issues are legitimate can help chiefs make effective use of social media while maintaining public support.

Further Reading & Resources

Association of Chief Police Officers and the National Policing Improvement Agency. "Engage: Digital and Social Media Engagement for the Police Service," www.acpo.police.uk/documents/LPpartnerships/2010/20110518%20LPPBA%20dm_engage_v61.pdf.

Connected COPS: Law Enforcement's Partner on the Social Web, http://connectedcops.net/.

Facebook. "Building your presence with Facebook Pages: A Guide for Police Departments." https://developers.facebook.com/attachment/PagesGuide_Police.pdf.

Her Majesty's Inspectorate of Constabulary (HMIC). "The rules of engagement: A review of the August 2011 disorders," www.hmic.gov.uk/media/a-review-of-the-august-2011-disorders-20111220.pdf.

IACP Center for Social Media, www.iacpsocialmedia.org/.

National White Collar Crime Center. "Criminal Use of Social Media," www.nw3c.org/research/site_files.cfm?fileid=f14a8af2-2087-446f-80e9-018dd573d526&mode=w.

Patridge, Justin (Senior Manager of Police Social Media, Local Policing and Partnerships for the Association of Chief Police Officers). "Social Media Handbook for Police," http://partridgej.wordpress.com/social-media-handbook-for-police/.

Public Safety Canada. "Social Media Sites: New Fora for Criminal, Communication, and Investigation Opportunities." http://publications.gc.ca/collections/collection_2012/sp-ps/PS14-5-2011-eng.pdf.

Twitter. "Guidelines for Law Enforcement," http://support.twitter.com//entries/41949-guidelines-for-law-enforcement#.

About the Cops Office

The Office of Community Oriented Policing Services (COPS Office) is the component of the U.S. Department of Justice responsible for advancing the practice of community policing by the nation's state, local, territory, and tribal law enforcement agencies through information and grant resources.

Community policing is a philosophy that promotes organizational strategies that support the systematic use of partnerships and problem-solving techniques, to proactively address the immediate conditions that give rise to public safety issues such as crime, social disorder, and fear of crime.

Rather than simply responding to crimes once they have been committed, community policing concentrates on preventing crime and eliminating the atmosphere of fear it creates. Earning the trust of the community and making those individuals stakeholders in their own safety enables law enforcement to better understand and address both the needs of the community and the factors that contribute to crime.

The COPS Office awards grants to state, local, territory, and tribal law enforcement agencies to hire and train community policing professionals, acquire and deploy cutting-edge crime fighting technologies, and develop and test innovative policing strategies. COPS Office funding also provides training and technical assistance to community members and local government leaders and all levels of law enforcement. The COPS Office has produced and compiled a broad range of information resources that can help law enforcement better address specific crime and operational issues, and help community leaders better understand how to work cooperatively with their law enforcement agency to reduce crime.

- Since 1994, the COPS Office has invested nearly $14 billion to add community policing officers to the nation's streets, enhance crime fighting technology, support crime prevention initiatives, and provide training and technical assistance to help advance community policing.
- By the end of FY2012, the COPS Office has funded approximately 124,000 additional officers to more than 13,000 of the nation's 18,000 law enforcement agencies across the country in small and large jurisdictions alike.
- Nearly 700,000 law enforcement personnel, community members, and government leaders have been trained through COPS Office-funded training organizations.
- As of 2012, the COPS Office has distributed more than 8.5 million topic-specific publications, training curricula, white papers, and resource CDs.

COPS Office resources, covering a wide breadth of community policing topics—from school and campus safety to gang violence—are available, at no cost, through its online Resource Information Center at www.cops.usdoj.gov. This easy-to-navigate website is also the grant application portal, providing access to online application forms.

About the Police Executive Research Forum

Founded in 1976, the Police Executive Research Forum (PERF) is a police research organization and a provider of high-quality management services, technical assistance, and executive-level education to support law enforcement and the criminal justice system. As a private, nonprofit organization, PERF was formed to improve the delivery of police services through:

- the exercise of strong national leadership;
- public debate of police and criminal justice issues;
- research and policy development; and
- the provision of vital management and leadership services to police agencies.

PERF has an extensive history of measuring all aspects of police agency performance, striving to find the best policing practices, and disseminating that knowledge to police agencies. PERF's groundbreaking projects on community and problem-oriented policing, racial profiling, use-of-force issues, and crime reduction strategies have earned it a prominent position in the police community.

PERF sponsors and conducts the Senior Management Institute for Police (SMIP), which provides comprehensive professional management and executive development education to police chiefs and other law enforcement executives. Convened annually in Boston, SMIP offers instruction by professors from leading universities, including many from Harvard University's Kennedy School of Government, as well as by leading police practitioners.

PERF has also developed and published some of the leading literature in the law enforcement field. Most recent publications include:

- 2011 Electronic Control Weapon Guidelines (2011)
- Labor-Management Relations in Policing: Looking to the Future and Finding Common Ground (2011)
- Managing Major Events: Best Practices from the Field (2011)
- Police and Immigration: How Chiefs Are Leading Their Communities through the Challenges (2010)
- Is the Economic Downturn Fundamentally Changing How We Police? (2010)
- Guns and Crime: Breaking New Ground By Focusing on the Local Impact (2010)
- Gang Violence: The Police Role in Developing Community-Wide Solutions (2010)
- It's More Complex than You Think: A Chief's Guide to DNA (2010)
- Law Enforcement Preparedness for Public Health Emergencies: An Executive Summary of the Resources Series (2010)
- Leadership Matters: Police Chiefs Talk About Their Careers (2009)
- Violent Crime and the Economic Crisis: Police Chiefs Face a New Challenge, Parts I & II (2009)
- The Stop Snitching Phenomenon: Breaking the Code of Silence (2009)

- Violent Crime in America: What We Know About Hot Spots Enforcement (2008)
- Police Chiefs and Sheriffs Speak Out On Local Immigration Enforcement (2008)
- Promoting Effective Homicide Investigations (2007)
- "Good to Great" Policing: Application of Business Management Principles in the Public Sector (2007)
- Violent Crime in America: A Tale of Two Cities (2007)
- Police Planning for an Influenza Pandemic: Case Studies and Recommendations from the Field (2007)
- Patrol-Level Response to a Suicide Bomb Threat: Guidelines for Consideration (2007)
- Strategies for Resolving Conflict and Minimizing Use of Force (2007)
- Police Management of Mass Demonstrations: Identifying Issues and Successful Approaches (2006)

For more information go to www.policeforum.org.

APPENDIX A:
Executive Session on Social Media and Tactical Law Enforcement Participants

October 13, 2011, Philadelphia, PA

Bay Area Rapid Transit Police
Chief of Police, Kenton Rainey

Baltimore County Police Department
Jordan Watts, Director of Legal Section

Charlotte-Mecklenburg Police Department
Chief of Police, Rodney Monroe

Chicago Police Department
First Deputy Superintendent, Alfonza Wysinger

City of Cleveland Law Department
Nancy Kelly, Asstistant Director of Law

City of Philadelphia
Mayor Michael Nutter

Dallas Police Department
Deputy Chief Randall Blankenbaker

Drexel University, College of Information Science and Technology
Professor Kristene Unsworth

Federal Bureau of Investigation, National Press Office
Supervisory Special Agent Jason Pack

Kansas City, Missouri Police Department
Major Roger Lewis

Las Vegas Metropolitan Police Department
Assistant Sheriff Raymond Flynn

LAwS Communications
Lauri Stevens, Social Media Strategist

Los Angeles Police Department
Commander Blake Chow

Metropolitan Police Department
Asstistant Chief of Police, Lamar Greene
Captain Wilfredo Manlapaz

Metropolitan Police Service (U.K.)
Inspector Jayme Johnson

Milwaukee Police Department
Chief of Police, Edward Flynn

Minneapolis Police Department
Chief of Police, Timothy Dolan

Montgomery County Police
Commander Luther Reynolds

New York Police Department
Deputy Inspector Steven D'Ulisse

Northeast Ohio Regional Fusion Center
William Schekelberg, Director

Office of Drug Control Policy, Executive Office of the President
Ellen Scrivner, National HIDTA Director

Philadelphia Police Department
Commissioner Chuck Ramsey
Deputy Commissioner Kevin Bethel
Deputy Commissioner William Blackburn
Deputy Commissioner Charlotte Council
Deputy Commissioner John Gaittens
Deputy Commissioner Patricia Giorgio-Fox
Deputy Commissioner Stephen Johnson
Deputy Commissioner Nola Joyce
Deputy Commissioner Richard Ross
Deputy Commissioner Thomas Wright

Prince George's County Police Department
Major Commander of Joint Analysis Intelligence Center, Christopher Cotillo

Strategic Policy Partnership
Bob Wasserman, Chairman

Tampa Police Department
Assistant Chief of Police, Marc Hamlin

TARGET Corporation
Mahogany Eller, National Public Safety Partnerships

Tayside Police Department (U.K.)
Deputy Chief Constable, Gordon Scobbie

Toronto Police Service
Deputy Chief of Police, Peter Sloly

University of Maryland, Department of Public Safety
Major Jay Gruber

University of Pennsylvania
Michael Morrin, Deputy Chief of Investigations
Maureen Rush, Vice President for Public Safety

U.S. Department of Justice, Community Relations Service
Knight Sor, Conciliation Specialist

U.S. Department of Justice, Office of Community Oriented Policing Services
Josh Ederheimer, Principal Deputy Director
Katherine McQuay, Assistant Director
Zoe Mentel, Policy Analyst

Vancouver Police Department
Superintendent Daryl Wiebe

APPENDIX B:
Site Visits and Interviews

Bay Area Rapid Transit (BART) Police Department
Chief of Police, Kenton Rainey

Los Angeles Police Department
Commander Blake Chow

Metropolitan Police (U.K.)
Detective Superintendent Steve Dower
Inspector Justin Leary

New York Police Department
Assistant Commissioner John McCarthy
Assistant Commissioner Kevin O'Connor
Captain Daniel E. Sosnowik
Deputy Chief Ruben Beltran
Deputy Inspector Steven D'Ulisse
Deputy Inspector Dennis Fulton
Deputy Inspector Michael Nemoyten
Sergeant Hukm Myles Moore
Christopher Apuzzo, Computer Operations Manager
Barbara Chen, Director of Media Relations

Tayside Police Department (U.K.)
Deputy Chief Constable, Gordon Scobbie

Toronto Police Service
Chief William Blair
Deputy Chief Peter Sloly
Director Mark Pugash
Meaghan Gray, Public Information
Sergeant Tim Burrows
Detective Constable Warren Bulmer

Vancouver Police Department
Chief Constable, Jim Chu
Sergeant Howard Chow
Detective/Constable Mark Fenton

APPENDIX C:
NYPD Operations Order

Use of social networks for investigative purposes—general procedure
September 5, 2012

OPERATIONS ORDER

SUBJECT: USE OF SOCIAL NETWORKS FOR INVESTIGATIVE PURPOSES – GENERAL PROCEDURE	
DATE ISSUED:	NUMBER:
09-05-12	34

1. Data contained within social network sites may assist law enforcement in gathering timely information in furtherance of crime prevention, preservation of public order, and the investigation of criminal activity, including suspected terrorist activity. These guidelines are promulgated, in part, to instill the proper balance between the investigative potential of social network sites and privacy expectations.

2. Therefore, effective immediately, when a member of the service requires the use of social network websites to conduct investigations or research, the following procedure will be complied with:

PURPOSE To conduct social network-based investigations and research.

SCOPE Data contained on the Internet within social network sites may assist law enforcement in gathering timely information in furtherance of crime prevention, including the preservation of public order and the investigation of criminal activity, including suspected terrorist activity. To effectively fulfill these duties, it may be necessary for members of the service to access social network sites using an online alias. No prior authorization is ever required for information contained on publicly available internet sources.

DEFINITIONS

EXIGENT CIRCUMSTANCES: For the purpose of this procedure, circumstances requiring action before authorization can be obtained, in order to protect life or substantial property interest; to apprehend or identify a fleeing offender; to prevent the hiding, destruction or alteration of evidence; or to avoid other serious impairment or hindrance of an investigation.

ONLINE ALIAS: An online identity encompassing identifiers, such as name and date of birth, differing from the user's actual name, date of birth, or other identifiers.

ONLINE ALIAS ACCESS: Internet-based searches involving the search and acquisition of information from sites that require an email address, password, or other identifiers for which an online alias is utilized.

PUBLIC DOMAIN DATA: Information accessible through the Internet for which no password, email address, or other identifier is necessary to acquire access to view or collect such information.

SOCIAL NETWORK SITE: Online platform where users can create profiles, share information, or socialize with others using a range of technologies.

PROCEDURE When a member of the service requires access to a social network website for investigative or research purposes:

MEMBER OF THE SERVICE

1. Confer with supervisor, if access to public domain data requires the use of an online alias/online alias access.
   a. No conferral or authorization is required for general research, topical information or other general uses that do not require the acquisition of an online alias/online alias access.

IF APPLICATION FOR ONLINE ALIAS DOES NOT INVOLVE SUSPECTED TERRORIST ACTIVITY:

SUPERVISOR

2. Evaluate request to determine whether an online alias would serve an investigative purpose, and if so, prepare **Typed Letterhead** requesting an online alias to bureau chief/deputy commissioner concerned.
3. Include on **Typed Letterhead**:
   a. Purpose for the request (i.e., type of investigation, etc.)
   b. Tax registry number of requesting member
   c. Username (online alias)
   d. Identifiers and pedigree to be utilized for the online alias, such as email address, username and date of birth.
      (1) Do not include password(s) for online alias and ensure password(s) are secured at all times.
   e. Indicate whether there is a need to requisition a Department laptop with aircard.
4. Review photograph to be used in conjunction with online alias, if applicable.
   a. Consider the purpose for which the photograph is being used and the source of the photograph.
   b. Attach a copy of the approved photograph and indicate on **Typed Letterhead** how photograph was obtained.
5. Forward request to commanding officer for review.

COMMANDING OFFICER

6. Review request(s) and consider the purpose and whether granting approval would serve an investigative purpose.
7. Endorse request(s) indicating APPROVAL/DISAPPROVAL within one day of original request and if APPROVED, immediately forward approval to bureau chief/deputy commissioner concerned, through channels, for informational purposes.
8. File copies of requests in command.

MEMBER OF THE SERVICE

9. Maintain record of online alias in case records management systems or appropriate Department records.

BUREAU CHIEF/DEPUTY COMMISSIONER

10. Maintain folder for each APPROVED online alias.
    a. Designate an administrator for the online alias.

IF APPLICATION FOR ONLINE ALIAS INVOLVES SUSPECTED TERRORIST ACTIVITY:

SUPERVISOR

11. Immediately contact Intelligence Division, Operations Desk supervisor and provide details regarding proposed investigation.

INTELLIGENCE DIVISION, OPERATIONS DESK SUPERVISOR

12. Determine if investigation should be conducted by the Intelligence Division and proceed accordingly.
13. Notify requesting supervisor to proceed with investigation if it has been determined that the investigation will not be conducted by the Intelligence Division.

SUPERVISOR

14. Comply with steps "2" through "10", as appropriate, if investigation will not be conducted by the Intelligence Division.

WHEN EXIGENT CIRCUMSTANCES EXIST THAT WOULD WARRANT THE IMMEDIATE USE OF AN ONLINE ALIAS:

SUPERVISOR

15. Confer with Intelligence Division, Operations Desk supervisor, if there is concern that the investigation may involve suspected terrorist activity.
    a. Comply with instructions from Intelligence Division, Operations Desk supervisor.
16. Confer with commanding officer/executive officer, if investigation does not involve suspected terrorist activity.
17. Instruct member of the service to proceed with investigation upon receiving APPROVAL from commanding officer/executive officer.
    a. Comply with steps "2" through "10", as appropriate, and include in **Typed Letterhead**, the circumstances that led to the determination of exigent circumstances.

ADDITIONAL DATA

LEGAL CONSIDERATIONS

During the course of an investigation, a member of service may need access to information regarding online accounts maintained by service providers. The federal Electronic Communications Privacy Act (ECPA) governs seizures of electronic evidence. Some information may be obtained with a subpoena; other information requires a special court order; and still other information requires a search warrant. Pertinent sections of the ECPA are as follows:

a. A subpoena is generally deemed sufficient to obtain information such as user information and payment records.

b. Electronic communications, such as email content, in electronic storage for 180 days or less may be obtained only after the issuance of a search warrant, and delayed notification to the subscriber or customer may be ordered if specifically requested in the search warrant application.

c. Electronic communications in electronic storage for more than 180 days may be obtained with a subpoena signed by a judge; however, notice must be provided to the subscriber or customer unless the electronic communications are obtained after the issuance of a search warrant allowing for delayed notification.

ADDITIONAL DATA (continued)

d. In anticipation of the issuance of a search warrant, a member of the service may send a request known as a "preservation letter" to an electronic service provider requesting the preservation of electronic records for 90 days, and extend the request for an additional 90 day period.

Note that particular service providers are known to ignore non-disclosure orders (i.e., some service providers will disclose the existence of a search warrant or subpoenas to a subject subscriber or customer.) In general, members of the service should consult with the Legal Bureau before seeking electronic communication through a search warrant or otherwise.

Data obtained through a grand jury subpoena or court order cannot be shared with other law enforcement agencies unless otherwise authorized.

OPERATIONAL CONSIDERATIONS

When a member of the service accesses any social media site using a Department network connection, there is a risk that the Department can be identified as the user of the social media. Given this possibility of identification during an investigation, members of the service should be aware that Department issued laptops with aircards have been configured to avoid detection and are available from the Management Information Systems Division (MISD). A confidential Internet connection (e.g., Department laptop with aircard) will aid in maintaining confidentiality during an investigation. Members who require a laptop with aircard to complete the investigation shall contact MISD Help Desk, upon APPROVAL of investigation, and provide required information.

In addition to using a Department laptop with aircard, members of the service are urged to take the following precautionary measures:

a. Avoid the use of a username or password that can be traced back to the member of the service or the Department;
b. Exercise caution when clicking on links in tweets, posts, and online advertisements;
c. Delete "spam" email without opening the email; and
d. Never open attachments to email unless the sender is known to the member of the service.

Furthermore, recognizing the ease with which information can be gathered from minimal effort from an Internet search, the Department advises members against the use of personal, family, or other non-Department Internet accounts or ISP access for Department business. Such access creates the possibility that the member's identity may be exposed to others through simple search and counter-surveillance techniques.

DEPARTMENT POLICY

The "Handschu Consent Decree" and "Guidelines for Investigations Involving Political Activity" (see Appendix "A" and "B" of Interim Order 58, series 2004, "Revision to Patrol Guide 212-72, 'Guidelines for Uniformed Members of the Service Conducting Investigations of Unlawful Political Activities'") require that any investigation, including investigations on social networks, by the New York City Police Department involving political activity shall be initiated by and conducted only under the supervision of the Intelligence Division. Accordingly, members of the service shall not conduct investigations on social networks involving political activity without the express written approval of the Deputy Commissioner, Intelligence. Any member of the service who is uncertain whether a particular investigation constitutes an "investigation involving political activity" shall consult with the Legal Bureau.

ADDITIONAL DATA (continued)	*Members of the service who have created and used online aliases prior to the promulgation of this procedure must submit a request to continue utilizing the alias in accordance with this procedure.*
RELATED PROCEDURES	*Citywide Intelligence Reporting System (P.G. 212-12)* *Guidelines for Uniformed Members of the Service Conducting Investigations of Unlawful Political Activities (Interim Order 58, series 2004)*
FORMS AND REPORTS	*Typed Letterhead*

3. Commanding officers will ensure that the contents of this Order are brought to the attention of members of their commands.

BY DIRECTION OF THE POLICE COMMISSIONER

DISTRIBUTION
All Commands

The use of social media is a relatively new phenomenon in policing. Development of formal policy on social media is generally lagging behind practice. A variety of legal, civil rights, and privacy-related issues regarding social media have been raised, but these issues have not yet been settled by legislatures or resolved in the courts. *Social Media and Tactical Considerations for Law Enforcement* summarizes discussions at a national conference of police executives on these issues, and analyzes the experiences of selected law enforcement agencies in the United States, Canada, and the United Kingdom that have shown leadership in advancing the use of social media for various purposes. Police agencies can use social media to facilitate two-way communications with the public to disseminate information, manage political demonstrations and other major events, obtain intelligence about "flash mobs" or rioting, and investigate crimes.

A joint project of:

COPS
Community Oriented Policing Services
U.S. Department of Justice

Police Executive Research Forum

U.S. Department of Justice
Office of Community Oriented Policing Services
145 N Street, N.E.
Washington, DC 20530

Police Executive Research Forum
1120 Connecticut Avenue, N.W.
Suite 930
Washington, DC 20036

To obtain details on COPS Office programs,
call the COPS Office Response Center at 800-421-6770.

Visit COPS Online at www.cops.usdoj.gov.

ISBN: 978-1-932582-72-7 e11331543
May 2013