Edited by:

J. Amber Scherer and Joseph A. Schafer

TRUST AND TRANSPARENCY ISSUES

IN THE FUTURE OF LAW ENFORCEMENT

VOLUME 8 of the Proceedings of the

Futures Working Group

Edited by J. Amber Scherer and Joseph A. Schafer

Suggested Citation:

Scherer, J.A., & Schafer, J.A. (Eds.). (2018). *Trust and transparency issues in the future of law enforcement: Volume 8 of the proceedings of the Futures Working Group*. Society of Police Futurists International.

Release Date: June 2018

Trust and Transparency Issues in the Future of Law Enforcement

Table of Contents

A WORD FROM THE PRESIDENT

This monograph represents another offering in a continuing series of works authored by members and affiliates of PFI's Futures Working Group (FWG). The foundation for this monograph was laid when the FWG was co-sponsored by PFI and the Federal Bureau of Investigation. The FBI's support of FWG spanned 2002

-2016 and that support allowed FWG to do valuable work. Although this monograph is not being co-published by the FBI, PFI gratefully acknowledges the FBI's support in this and many other work products written during more than a decade of strong collaboration.

The contributions contained in this monograph are intended to spark ideas and incite creativity in responding to the future challenges and opportunities that policing and the criminal justice community must confront. As with most monographs, this is a working document. It is not intended to be the final word or definitive perspective concerning the topics discussed. Rather, these contributions are designed to foster further discussion and consideration of possible, probable, and preferable future directions for policing. In this vein, the current papers offer a perspective on the critical issue of how trust and transparency relate to the future of policing. We hope you find this, as well as past and subsequent FWG white papers, to be useful.

Dr. G.M. Cox

Tarleton State University

2017-2018 President of PFI

Understanding Trust and Transparency in Contemporary Policing

Joseph A. Schafer & John P. Jarvis

This volume of working papers considers the role of trust and transparency in contemporary and future police organizations and operations. Trust and transparency are of importance across organizational contexts, particularly within government services. Research suggests that people who perceive decision making to be just and based on appropriate procedures are more likely to see the decision maker and their decisions as legitimate (see Sunshine & Tyler, 2003; Tyler & Huo, 2002; Tyler, 2010). When people trust decision makers, see them as having legitimate power, and believe they use appropriate pathways to selecting specific choices, they are more likely to obey and cooperate. This has clear importance and implications for the criminal justice system, where obedience and cooperation are central to ensuring efficacious and expedient processing and outcomes. These issues are of central importance in government services, especially within policing. Indeed, much of the controversy surrounding US policing in recent years is arguably rooted in distrust and perceived lack of transparency in police processes, high-profile police-citizen encounters, and the broader oversight of police organizations and operations. The recommendations of the President's Task Force on 21st Century Policing (2015) repeatedly touch on the need to make policing more transparent and to build greater trust between the police and the communities they serve.

Officers and departments frequently make choices that are not popular with citizens. Those being arrested are rarely pleased with that outcome. Dr. Tyler's work suggests that, in the aggregate, there will be more support for, and compliance with, police decisions of all types when citizens perceive the police are just and fair.[1] Trust and transparency are presumably central pathways to fostering the belief that officers and departments are operating in a manner that is fair, just, and legitimate.[2] When citizens trust the police and see that operations

[1] Certainly this will not always be the case. Any group or individual can only do so much to ensure compliance and obedience, particularly when decisions are controversial, unpopular, or impactful.

[2] This does not suggest that other pathways do not exist. Trust and transparency are important, but not the exclusive mechanisms for engendering public support and compliance.

are handled in an appropriately visible manner, it will be easier to perceive the police and their authority as being legitimate. When communities trust there is appropriate oversight of their police, trust that officers are held sufficiently accountable for their decisions, and perceive that organizations operate with an appropriate level of transparency, those communities should, in theory, be more trusting of the police when critical and controversial events occur. This should translate into greater support, cooperation, and deference to police authority and power.

In the context of this volume, trust relates to the ability of those inside and outside the organization to have a degree of faith and confidence in the abilities and decisions of those in control. Trust suggests that decision makers can engender a sense they are reliable, dependable, and worthy. Trust might often suggest a degree of predictability. In policing contexts, citizens who believe their police department is diligent, hardworking, and professional would be expected to show greater support for that agency and its decisions. Trust also has an internal dimension; police officers may (or may not) have a degree of trust in the motivation, competence, and abilities of their supervisors.

In the context of this volume, transparency captures the degree to which decisions are being made in a visible fashion. To what extent are operations subject to review and scrutiny by outsiders? To what extent are the choices of decision makers readily evident? As bureaucratic entities, police organizations and officers make a wide range of decisions on a daily basis. Traditionally the forces and factors influencing those decisions have existed in a rather opaque environment. It has been easy to see the inputs (crimes reported to the police; fiscal allocations to the police department) and the outputs (crimes reported by the police; the budget use to "spend down" the defined budget), yet understanding what happened in between (the 'why' questions…why were some reported crimes 'counted' while others were not?...why did the agency decide to fund a drug suppression unit and not a drug education program?) has been far more elusive. Transparency speaks to efforts intended to shed more light on 'why' questions by helping provide an understanding of how agencies and officers make decisions, rather than merely relying on speculation and inference.

Trust and transparency are related concepts that both seem likely to condition and shape the level of confidence in, and support for, the police. These two concepts are not, however, identical. An organization can enjoy a high degree of trust without being particularly transparent; the converse might also be true. Likewise, we need to consider the trust and transparency as forces existing both within (internal) and outside (external) police organizations. The former refers to the nature of relations between an agency's leadership and its front-line personnel. Internally an agency might be quite open in how it operates, makes decisions, allocates resources, etc., while those outside the organization may have little understanding or sense of transparency.

Likewise, an agency's executives might behave in such a way that internal trust is quite high; in so doing, external trust might be damaged. For example, former LAPD Chief Daryl Gates had a well-established reputation as a 'cops cop' that presumably generated a high degree of internal trust. Gates was a staunch defender of officers and their actions during controversial situations. It would be expected officers greatly trusted Chief Gates as their leader because they knew he 'had their back' if they were being subjected to public scrutiny over how they were policing the community. At the same time, we might expect that citizens often felt disenfranchised from LAPD and its personnel, questioning whether Chief Gates and other officials were willing to hold officers to high standards of performance and accountability (see Reese, 2005).

Why should organizations value and pursue trust and transparency? Most importantly, police organizations are representatives of the state and are granted tremendous power and authority. With that comes tremendous responsibility to the public and external sovereigns (i.e., the city, county, state, or federal officials overseeing an agency). If police organizations are going to be effective in controlling crime, they must have the confidence, support, and cooperation of the public they serve. When citizens perceive government agencies and agents are acting in a fair and just manner, they are more supportive, compliant, and obedient (Tyler, 2010). By extension, we would expect this behavior results not only in more orderly communities, but, by extension, in citizens who are more willing to cooperate with the police in

the investigation of specific crimes and in broader efforts to improve the quality of living in a jurisdiction. Two mechanisms that should facilitate these processes are trust and transparency.

Conversely, if agencies do not value being trusted by the public and being transparent in their operations, they will not enjoy the same ability to influence crime and community conditions. The distinction between agencies that do not and do see value in trust, transparency, justice, and legitimacy is the former see policing as something done *to the public*, while the latter sees it as something done *with the public*. This does not suggest that agencies operating with an emphasis on trust and transparency will experience a panacea in which citizens always support the police and cooperate with officers. Rather, it suggests that any benefits perceived to be associated with de-emphasizing transparent police operations or emphasizing control over trust are short-term gains. In the aggregate, emphasizing trust and transparency (which will not always be easy) is both philosophically 'right' and will do the most to advance the interests of the agency and community. Furthermore, emergent technologies are increasingly forcing transparency on agencies and police personnel; rather than fighting that reality, agencies would be better served to seek to maximize the potential of that trend.

Matters of trust and transparency are not limited to how police agencies and personnel intersect with their external environment. Trust and transparency are key considerations when seeking to understand the nature of police organizations, operations, and leadership. Parallels have been drawn between Tyler's works on how the police interface with their external environment by examining the level of trust, transparency, and perceived justice within police organizations, as well (Nix & Wolfe, 2016; Rosenbaum & McCarty, 2017). Part of the embedded logic driving this research is that officers should not be expected to demonstrate procedurally just and trustworthy policing toward the public if they do not enjoy organizationally just and trustworthy treatment by their employing organization. If police executives expect their officers to police with an eye for citizen perceptions, trust, legitimacy, and fairness, those executives must first treat employees with an eye for those same principles (Carr & Maxwell, 2017; White & Kyle, 2017). Officers want to see a workforce where decisions are fair, equitable, and compliant with governing policies, procedures, and laws. Officers want a workplace that does

not issue arbitrary and inconsistent discipline, where promotions are based on merit and not favoritism, and where accountability systems are viewed as treating officers fairly and justly.

Within a 2x2 matrix (see below) contrasting the internal and external dimensions of trust and transparency, an agency might be assessed as high, low, neutral, or negative within each of the 4 cells. Assessments would be expected to vary both across agencies and also across time. For example, the external trust in LAPD would presumably be different today than it was in the early 1990s near the end of Chief Gates' tenure. The former KGB would likely have been rated as being negative in all 4 cells. Presumably front-line personnel were nearly as fearful of the agency as were citizens, knowing that methods were dubious, evidence standards non-existent, and that control, not justice, was the ultimate objective.

	Internal	External
Trust		
Transparency		

One hundred years ago, the Berkeley PD under August Vollmer (see the essay by Schafer in this voume) was very high on internal trust and transparency, at least according to the lore and limited historical evidence. Based on the latter it is less clear if the model Vollmer used generated external trust and transparency, though that outcome would seem probable. It would generally be expected that agencies that have healthy internal operations would probably fair well on external trust and transparency. While that is not an automatic outcome, officers cannot be expected to operate in support of a high degree of external trust and transparency (if that outcome is valued) without seeing that behavior modeled internally. If leaders do not treat personnel in a way that demonstrates how to engender internal trust and ensure internal transparency, it would be unlikely to routinely see front-line personnel operating in a way that would facilitate high levels of external trust and transparency.

It can be very difficult for executives/agencies to simultaneously and continuously excel in all four cells of the 2x2 matrix. Sometimes being high in one area will reduce and agency's

standing in another area, at least temporarily. If an agency is externally transparent in admitting to a scandal or operational problems, it might temporarily work against the public's trust in that agency. Over time, however, the honesty and external transparency of this approach would be expected to result in more public support and trust. Furthermore, attempting to conceal internal issues (low external transparency) often compounds the depth of a scandal and its fallout. What executives need to hope is that over time and in the aggregate they can find ways to excel in all 4 cells of the table, realizing that in some contexts a victory in one area will be a defeat in another. Perfection will not be possible, but trying to hide/suppress simply yields false victory. And in an increasingly transparent world, it is becoming increasingly difficult to hide/suppress, making voluntary transparency all the more important in order to reduce damage to trust (recognizing legal matters complicate complete and timely transparency when situations are still being investigated).

The focus of the present volume is offering a mixture of perspectives on how trust and transparency can be understood in the current and future world of policing. The authors offer a variety of views on how policing practices might intersect with technology and contemporary social norms to create new expectations officers and leaders must understand and address. The essays do not seek to provide a definitive and final word on matters of trust and transparency. Rather, they seek to offer thoughtful and thought provoking commentaries and insights to help guide policing to a future where trust and transparency are viewed as tools to enhance police operations and public service, not liabilities or risks in need of management or mitigation.

References

Carr, J.D., & Maxwell, S.R. (2017). Police officers' perceptions of organizational justice and their trust in the public. *Police Practice & Research*, DOI: 10.1080/15614263.2017.1387784.

Kyle, M.J., & White, D.R. (2017). The impact of law enforcement officer perceptions of organizational justice on their attitudes regarding body-worn cameras. *Journal of Crime and Justice, 40*(1), 68-83.

Nix, J., & Wolfe, S.E. (2016). Sensitivity to the Ferguson Effect: The role of managerial organizational justice. *Journal of Criminal Justice, 47*, 12-20.

President's Commission on 21st Century Policing. (2015). *Final report of the President's Task Force on 21st Century Policing.* Washington, DC: Office of Community Oriented Policing Services.

Reese, R. (2005). *Leadership in the LAPD: Walking the tightrope.* Durham, NC: Carolina Academic Press.

Rosenbaum, D.P., & McCarty, W.P. (2017). Organizational justice and officer 'buy in' in American policing. *Policing: An International Journal of Police Strategies & Management, 40,* 71-85.

Sunshine, J., & Tyler, T. (2003). The role of procedural justice and legitimacy in shaping public support for policing. *Law and Society Review, 37*(3), 513-547.

Tyler, T.R. (2010). *Why people cooperate: The role of social motivations*. Princeton, NJ: Princeton University Press.

Tyler, T.R., & Huo, Y.J. (2002). *Trust in the law: Encouraging public cooperation with the police and courts*. New York: Russell-Sage Foundation.

Transparency, Truth, and Perception: A Complex Relationship

Gene Stephens

Transparency has become both a buzzword and sometimes a reality in 21st century government, including the public safety arena. A 2012 presidential memorandum from the White House Press Office declared transparency the policy of the United States government, defining it as "to disclose information rapidly in forms that the public can readily find and use," and holding such a policy "promotes accountability and provides information for citizens about what their government is doing." Others call for a broadening of transparency from "show us what you have done" to "let me participate in what you're doing while you're doing it" (www.granicus.com/transparency). The latter definition corresponds to the approaches advocated in neighborhood-driven policing, reformulated community policing, and even network centric policing.

While everyone stands firmly in favor of 'truth' in all dealings in a transparent environment, the search for truth is much more complex than it might first appear. Anyone who has been at the scene of a domestic dispute or street brawl is aware that those at the scene readily expound numerous versions of 'the truth'. Even after collecting all versions and physical evidence, truth often remains elusive. Beyond this, evidence (from eyewitness testimony to forensic) often results in conflicting interpretations; the wheeling and dealing within the court process often ignores or obscures 'truth' even further.

A relatively new discipline, Popular Culture (Bailey & Hale, 1998) views 'perceptions' as more important than truth in the search for 'reality' within any culture. It goes so far as to posit that perceptions are the major factor in determining 'truth' and even shape what is accepted as truth. For example, the myriad CSI television programs provide a perception that forensic evidence is always available, can be collected and analyzed quickly, and is necessary to provide swift and fair justice. Whereas the reality is that such evidence is sometimes available and can be collected by trained, competent investigators, often such evidence has been destroyed

before authorities arrived. Even if found, few crime laboratories can provide testing and analysis in hours or days—usually it is weeks or months— and is done at a facility many miles from the crime scene. But the perception has led to the reality that numerous cases are lost because forensic evidence is not forthcoming and jurors (many of whom are CSI fans) expected it and are suspicious about why it is missing. Thus the perception is more important than the truth in creating reality.

Transparency requires "openness, accountability, and honesty." Transparency is to be judged by the "depth of access" allowed and the "depth of knowledge" provided to the public (sunshinereview.org). Agencies that score best would not only allow access, but would provide "proactive disclosure" rather than waiting for individual requests for public records. Thus providing transparency and truth supported by public perception is far from simple; the complex relationship among these and other factors must be studied and deciphered if any success is to be expected. It may be that the process is more important than the results and that process must follow from careful analysis and attention to policy direction that has the best chance of leading to the desired outcomes.

Transparency is difficult in any public institution, but has special problems in public safety agencies. How much information can or should be made available in cases where suspects are seeing and hearing in real time the same broadcasts/webcasts/blogs as everyone else? When must information be withheld to protect the identity and well being of undercover officers or informants? How much of delicate negotiations with kidnappers or terrorists can be divulged without putting lives at risk? Can victims' names be withheld until next of kin are notified; is it even possible to withhold such information in light of the omnipresent media? Is a witness protection program even possible under this definition or does openness require full disclosure of the witness' whereabouts and circumstances? How much can be released about interagency haggling for budget dollars without sabotaging any chance the public safety mission can be accomplished? For that matter, can there be any place left for behind-closed-doors meetings where authorities can candidly discuss issues rather than politically posture for media and/or attending citizens?

Even when transparency is the intent of agencies, truth does not necessarily result from openness. Seemingly simple truths—who did what to whom and why—are associated with doubts and disputes in most cases. Keeping the public informed as soon as possible in the interest of transparency can result in what turns out to be dissemination of misinformation, which can run counter to the goal of establishing trust with the community. Still, transparency is not a choice; it occurs in our hyper-connected society—again, not necessarily revealing truth.

Truth for purposes of this discussion is better understood as a relative term, rather than an absolute. Good investigators realize they collect evidence, not proof, and they support theories, not fact. Popular culture literature posits that truth is a product of perception. That perception is more important than truth and, indeed, is the source of truth. The preeminence of perception is basic to the psychological theory of cognitive dissonance, which holds that when an individual is faced with dissonant (conflicting) cognitions (beliefs), discomfort is created and the individual seeks to reduce or eliminate the dissonance, usually in the easiest manner possible (Festinger, 1957). In most cases, the individual accepting the cognition that is closest to matching his/her established beliefs removes the conflict. This chosen perception thus becomes his/her truth. Given the same choice, another person might find the opposite or a different cognition more in harmony with his/her belief system and thus adopt that perception, which then becomes his/her truth. Thus the same set of 'facts' becomes a separate truth for different people.

This approach is so ingrained in most people that they choose their sources of information by how closely it matches their preconceived beliefs, thus avoiding challenges that could result in cognitive dissonance. This is particularly evident in the public safety arena, where a disagreement or confrontation between a citizen/suspect and a public safety officer often can result in various citizen groups taking sides in the dispute based on past experience and perceptions/beliefs about everything from character of police, character of the ethnic group of the suspect, character of the age group of the suspect, time of day the event occurred, etc. While stereotyping often is unfair and not supported by the preponderance of available evidence, it is widely used by all as an efficient way of managing information and making

decisions; cognitive dissonance occurs when those stereotypes are challenged. After the event, individuals will seek out others and/or media (e.g., talk shows, websites, blogs) that support and thus reinforce their perceptions—their truths—about the dilemma.

Thus transparency does not equal truth, nor does transparency guarantee that the openness of providing information will result in the discovery of truth. Still, the openness and sincerity with which the process is attempted can result in the development of the trust and dialogue that is an essential prerequisite to success in any community policing effort. Transparency, truth, and perception are inextricably entwined in a complex relationship that public safety officials must decipher in order to develop fair and effective policies that serve the unique characteristics of each individual jurisdiction.

References

Bailey, F. Y. & Hale, D. C. (1998). *Popular culture, crime, and justice*. Belmont, CA: Wadsworth.

Festinger, L. (1957). *A theory of cognitive dissonance*. Stanford, CA: Stanford University Press.

www.granicus.com/transparency

www.sunshinereview.org

The Role of Leadership in Fostering Truth and Transparency

Richard W. Myers

Transparency Shapes Culture

The leader's role in organizations is often targeted for speculation, both in overstating and underestimating importance. Having served as a leader for over 25 years in multiple police agencies, this author can attest that day-to-day decision making becomes less and less of the routine of the leader as organizations grow in size. The impact that one man or woman can have on a group of employees has many variables, including the nature of their role, experience, the culture of the organization, the history of relationships, and the perception of power, whether genuine or contrived. With respect to organizational culture, however, there is no denying the critical role that the CEO plays. Over time, members of an organization will reflect the cultural tone set by the leader, either by embracing the principles and behaviors modeled, or acting out the conflict that arises from poor leadership. For example, leaders who demonstrate active collaboration with outside organizations generally will see an overall climate of collaboration; leaders who are insular will, conversely, see partitioned, protective, and survival behaviors within their membership. One area in which the leader's example sets a strong organizational expectation is transparency and truthfulness. A strong example of truth and transparency by leadership has implications both internal and external to the organization.

Internally, transparency and truthfulness shape and define elements of organizational communication. When a leader speaks directly, honestly, and is not afraid to reveal all sides of an issue of importance to the membership, it empowers others to exchange information in a similar manner. With time, honest and open communication becomes an expectation, and peers are likely to hold each other highly accountable for sustaining this communication style. Leaders who own up to the truth and the price tag that comes with it are much more credible than those who avoid it; those leaders who seek to conceal or deny face an even greater loss of credibility, and with it, the loss of legitimacy.

Externally, particularly in high visibility organizations such as police departments, leaders who are forthright convey to the outside world that honesty and transparency define how the organization will treat customers, critics, constituents, and even their own employees. Nowhere is this more critical than in times of crisis and when an organization makes a mistake. No organization is impervious to error; when high-risk organizations err, however, the expectation for accountability is high. Former Chicago Police Superintendent Terry Hilliard was known for the expression: "If you mess up…. fess up and clean up." Ultimately, a CEO's behaviors will largely shape the organization's reputation for trust and legitimacy.

Despite the wide-ranging conjecture of the role of the police CEO, most police leaders are in the business of shaping organizational culture. The CEO will, from the time of their appointment, constantly assess those cultural elements that are positive and should be strengthened and those that need changing. Successful cultural change is most likely when the CEO engages the employees in the process and maintains a pace that is challenging yet attainable for the membership. A CEO who arose from within the ranks has perceptions to overcome, related to personal history and some who might believe their loyalty to history trumps the need for change. A CEO appointed from the outside has the challenge of quickly assimilating and understanding cultural nuances to which they have not been previously exposed. In both cases, cultural change involves 'sacred cows'; CEOs must be sensitive in communicating any need for change, pacing the change appropriately, and significantly engaging the employees.

Internal Transparency

Focusing internally in the organization, an almost universal phenomenon in police organizations is a varying level of inherent mistrust between the rank and file employees and the CEO. An absence of this mistrust is the exception, despite the fact that each and every police organization has its own unique culture. In any industry, including policing, there are two kinds of culture, however. The first may best be described as The Police Culture, containing elements that seem universal in almost all police organizations. These cultural elements are

perpetuated by both the nature of police work and the strong networking within the industry. An example of an almost universal dynamic of The Police Culture is the significant impact that a line-of-duty death has on an entire organization and the surrounding regional fraternity of police. The death of an officer almost always brings a sense of closeness, the result of the shared pain and reality of the dangers of the profession. It is a necessity and expectation of The Police Culture to amass a great gathering of police from far and wide, to express the collective grief and compassion for the surviving co-workers and family members.

Locally, the second kind of culture is that which is unique to each and every organization, no matter the size. Thus, the industry 'Culture' and the local 'culture' combine to form that which is truly individual and unique. In the above line-of-duty death example, the local culture will dictate some of the unique nuances of the funeral, along with the lingering psychological impact on the department members, and how involved the department will be with the surviving family. The local culture may allow for an analytical dissection of the incident so that the lost life may continue to provide officer safety lessons for the peer group, while in other local cultures, it may become taboo to critique any actions of the departed.

Both kinds of cultures work to feed any present element of mistrust between labor and management. Many agencies have an historic 'mushroom syndrome', wherein the employees feel 'kept in the dark and fed compost,' even if this is contrary to the style of the current leader. Industry-wide, there is a common perception that the CEO is far removed from the 'real work' of the street officers, and there often is a factual basis for that sense. As written previously by the Futures Working Group, strictly hierarchical organizations are subject to the filtering that comes from multiple layers of supervision, distorting messaging so that results rarely align with the stated 'truth' (Jackson, Myers, & Cowper, 2010). And, in most organizations, the rumor mill operates at a speed with which formal communications cannot compete. Collectively, these cumulative factors breed a degree of mistrust.

Conscientious CEOs will invest significant effort to overcome this inherent mistrust and their direct messaging to employees is a strong opportunity for transparency. No matter what size organization, CEOs who meet directly with groups of employees enjoy an unfiltered

experience that comes with immediate feedback. As a newly appointed police chief from outside the organization, I found it extremely helpful to schedule time to attend shift changes at each of the regional police stations under my command. The attending officers began to know me as the leader AND as a person. The interactions provided a platform to directly convey the leader's intent and vision, as well as listening sessions to hear employee concerns directly. Direct distribution of written communication from the CEO will be free from filtering as well; however, sometimes a CEOs message does not connect well directly with line level employees without some degree of loyal and accurate translation from middle management. Middle managers will know the local culture and how to best translate any messages that may be viewed as esoteric or too academic to relate to line level employees.

Filter-free written communication is more likely to occur if the CEO relies on highly repetitive and clear talking points, resulting in supervisors and middle managers 'carrying the flag' as they fulfill the informal translation role. From the day of my appointment as the new chief from outside the organization, I began talking about four straightforward key themes of my leader's vision. I repeated those themes along with expanded definitions throughout the term of my tenure. Over the course of time, it was apparent that others referred to those themes as they discussed programs, tactics, and concerns within the organization. The risk with any level of direct communication between the leader and the troops is that it can be threatening to middle managers; unless the managers understand and embrace this strategy, they may resist or even sabotage while engaging in survival behaviors. Ultimately, leaders who are willing to put aside ego to explain their actions and decisions will increase both transparency and trust.

Internal transparency comes with both benefits and costs. The benefits include an increased sense of trust among and within employees. The CEO is better able to set a vision and philosophy for the entire organization to follow. Consistent truthfulness and transparency by the CEO is usually accompanied by increased respect, a key ingredient for strong followership. The CEO needs to be prepared for the costs. Especially early on, some employees will test the new transparency, ask tough questions, and demand explanations. Some will studiously track

what has been said and call out any deviation from previously stated facts, even if unintentional. Consistency becomes critical in this environment. Sometimes transparency unavoidably sheds light on individuals; rank and file may overlook or even view this with glee when it adversely impacts someone of rank or authority. However, when a line level employee suffers, it may result in an overall organizational rejection or revolt. Whenever a CEO begins to lift the veil away from an organization's 'dirty little secrets' there will likely be pushback, especially if it results in inquiries into long standing practices, policies, and other elements that comprise the sacred culture.

External Transparency

Even when some of the previously mentioned pushback spills out into the external environment, practicing strong external transparency provides a highly effective means for both the CEO and the entire organization to tell their story to the community. While the relationship between the media and the police varies from community to community, almost all organizations will lament a certain degree of spin and distortion by some local reporters. Many organizations are generating their own news through the proactive use of social media; this offers a direct and unfiltered means to demonstrate trust and transparency. It is easier to attack anonymity than it is the known. Proactive and direct public communication, bathed in transparency, increases public awareness and familiarity with their local police, in turn increasing trust. Some police agencies are strategically advancing in the path of private sector marketing, developing a recognizable brand and even direct marketing their story and outreach to specific segments of the public that may benefit from a stronger relationship with the police. Increasing trust with minority groups, mental health providers and consumers, schools, businesses, and underrepresented segments of society can only benefit the partnership between the police and the community. While serving as chief in a large community, I developed advisory committees from within the minority communities and the faith communities to provide a direct exchange of information. Over time, the mutual trust level rose significantly; this required a level of frankness that at times was uncomfortable for the

attending command staff, but provided a timely modeling opportunity as a leader to demonstrate the value of transparency. The willingness to reveal aspects of the police organization that have historically been inaccessible can reverse prior media driven perceptions and grow trust. Genuine transparency, however, is not simply marketing the good news. The previous quote about 'if you mess up, fess up' highlights the equally important responsibility to acknowledge mistakes, lessons learned, and proposed solutions.

External transparency carries potential costs, as well. The initial increase in transparency may include revealing previously withheld errors or misbehaviors; in the short term, this may increase mistrust as the public ponders why the information was not released previously. To strengthen my agency's compliance with public accountability standards, our agency began publishing annual Internal Affairs Investigation summary data. Members of the command staff were highly reluctant to publish the summary data, rightfully concerned about stimulating increased media scrutiny. Over time, the media keys in on the trends up or down and less on specific cases, except for the more egregious and titillating examples.

Some employees may not readily accept or appreciate a leader's airing the organization's 'dirty laundry,' resulting in longer term resentment and pushback. At the extreme, no matter what degree of transparency exists, renegade employees at some agencies have embarked on their own external transparency efforts. Examples in many cities include posted comments at the end of web-based news stories blogged by those identifying themselves as police employees. Even more severe are social media posts and controlled by destructive current or former employees who may weave a thread of truth among their extreme perceptions and misstatements. Such content poses a significant challenge to the CEO who seeks internal and external transparency; on one hand, they do not want to legitimize the blogs by acknowledging their existence, and on the other hand, ignoring them provides no counter balance.

Finally, an unintended consequence of increased external transparency may result in the 'give them an inch and they'll take a mile' syndrome. One or more members of the media may never be satisfied with the increased flow of facts and information, instead increasing their

demands for more and more probative and sensitive information. Even the most transparent-minded CEO recognizes that in the policing business, employee safety and certain missions require strict confidentiality.

Future Considerations on Transparency

CEOs who are hesitant to embrace the spirit of transparency may have no choice in the future. Open source information is increasing in speed of availability and is becoming ubiquitous for any and all, including police organization members. Any attempts to keep information from employees will only drive them to seek alternative sources; this preempts the leader's ability to remove filtering that might alter the perceptions of the employees. Conversely, the CEO who has a clear vision of advanced transparency could turn to social media and similar technologies as a means to proactively get information out to employees ahead of the rumor mill.

Despite the relentless pursuit of faster dissemination of information, speed will need to be balanced with accuracy and completeness. Information in policing is dynamic; the 'truth' often changes as more facts are known. The media tends to overlook this dynamic in policing, resulting in the appearance of uncertainty by the police or even intentional deceit. How police employees explain and update dynamic information will largely influence if the transparency helps or hinders increased trust. As social media has exploded, attempts to keep information secret or proprietary have become futile. Those who cling to the historic ability to conceal unpleasant circumstances are at increased risk of irrelevance. Future leaders will demonstrate skill at transparency coupled with accountability.

Finally, empowered employees are most likely to behave with a level of external transparency. The role of the CEO to firmly ground the organization and its members with values and principles and define the boundaries of acceptable behaviors is crucial in this environment (Myers, 2007). In all quality organizations, a climate that allows growth through innovation and even mistakes serves to empower employees and increase their competencies.

A transparent police organization will not try to disavow or cover up mistakes; rather, it will reward employee growth and build trust with its community through education and accessibility.

References

Jackson, J., Myers, R., & Cowper, T. (2010). Leadership in the net-centric organization. In J. Schafer & S. Boyd (eds.), *Advancing police leadership: Considerations, lessons learned, and preferable futures* (pp. 138-149). Quantico, VA: Futures Working Group.

Myers, R. (2007). From pyramids to networks: Police structure and leadership in 2020. In J. Schafer (ed.), *Policing 2020: Exploring the future of crime, communities, and policing* (pp. 487-519). Quantico, VA: Futures Working Group.

Private/Public Partnerships for Fostering Trust within the Community

Alan Youngs

One need only review the events in Aurora, Colorado, during the Aurora theatre shooting on July 20th, 2012 to see an example of how police can build trust in the community in times of crisis. A police response of 90 seconds after the first 911 call and the ability to mobilize a large number of officers for rapid response kept the loss of life from reaching even higher levels. Twelve people died and 58 were injured. Communication between departments and districts were second to none. The responding officers exemplified professionalism. The EMTs and private sector medical personnel worked with the police as a team and were all at their best. The leadership from the Aurora Chief of Police Dan Oates was superb. While the media clamored for details, Chief Oates gave them important facts, but clearly declared that information pertinent to the case would not be released lest the case be jeopardized and justice not be delivered to the victims. He was calm, he was informative, he was compassionate, and he reassured the public that their safety was of utmost importance.

It was obvious in this horrific situation, as with others such as September 11th, Columbine, and Las Vegas that the police proudly displayed the training they had received to protect and serve. Still, as the old adage goes, people love and want the police in crisis. Trust can be eroded when transparency and truth are lacking. Transparency and truth should always be part of daily police work. It is not, as with Chief Oates, always telling everything that is happening, but communicating in a way that people understand the reasons information is withheld. It is not just what is communicated but how it is communicated. Transparency extends to police budgets, salaries, pensions, training, and expertise. It is admitting that the private sector can in some cases do as good or better a job at a lower cost. It is keeping budgets, salaries, overtime, and pension programs before the public eye because they can be and should be justifiable.

Everyone suffers in an economic crisis. There needs to be balance between the private and public sector. Governments worldwide are viewed as wasteful and often corrupt. Public

workers are viewed as being rewarded more than the private sector worker, their pensions, medical benefits, and salaries untouched by market conditions. This is not always true, but the perception remains and cuts are being demanded nationwide to public worker benefits and bargaining powers. Building and maintaining relationships of trust between law enforcement and the communities they serve is the cornerstone of successful policing. The importance of trusting relationships will prevent acts of crime and terrorism. With the evolving nature of immigrant and minority communities, community policing is described as a successful strategy that can be used by law enforcement to collaborate and partner with local communities. The building and maintenance of trust takes a great deal of continuous effort.

Unfortunately, the ethical work of thousands of local law enforcement officers is easily undone by the actions of one unethical officer. Often the indictment of one seems like an indictment of all. The challenges faced must be addressed with law enforcement and communities to develop relationships of trust. For law enforcement agencies, it means that meaningful dialog and collaboration with communities needs to occur in a manner that increases legitimacy of the agency in the eyes of that community. For communities, their leaders and representatives must collaborate with law enforcement and share responsibility for addressing the problems of administration and budgeting, as well as crime and terrorism prevention.

There are nearly 18,000 state and local law enforcement agencies in the United States employing over 700,000 full-time sworn personnel (Reaves, 2011). It has been estimated that there are almost 2 million individuals engaged in some form of private security within the U.S. Private security companies offer a wide variety of services from basic unarmed guards to sophisticated computer security. Over 80% of our country's infrastructure (water, power, transportation, etc.) is protected by private security. Public law enforcement has the legal mandate to enforce laws and while some efforts have been made to adopt a prevention model, in recent years, they have more frequently followed the enforcement model. Private security generally follows a prevention strategy. Cooperative efforts among the public, police, and the private sector are not new. However, since the attack on September 11, 2001, there has also

been a keen interest in public/private partnerships that would increase homeland security. Collaboration and information sharing between both will be critical to any success we will have in combating terrorism.

Building and Sustaining Trust Can Be Difficult

How the community perceives law enforcement depends on each police department. How the department interacts with its citizens, how accessible it is to the community, and how it manages internal issues are integral to the profession overall. It is for these reasons that building and maintaining community trust is the hallmark of effective policing. The public's trust in law enforcement may be fleeting if police executives do not continually reinforce sound, ethical policies and procedures to agency personnel and to the public. Maintaining honor and integrity within the organization will result in building and sustaining a trusting relationship between the public and the police.

The rapidly changing demographic face of America is changing the landscape of the communities that law enforcement agencies serve. The United States is a nation brought together under the promise of liberty, equality, and opportunity, founded on principles and the rule of law. The police are the guardians of the laws and principles and serve the noble cause of preserving our democracy 24/7, 365 days a year on the front lines of the United States, the streets and homes of America. Unlike the military that defends the United States from foreign threats, the police mission is to proactively defend and preserve a chosen way of life: democracy. As such, the police being the most visible representatives of government in society are the most crucial element of a just, fair, and free nation.

The Future of Public/Private Partnerships

Today's police departments are under monumental pressure to reduce crime with fewer resources.[3] Privatization of law enforcement is not a new concept (Bayley & Shearing, 2001). France led the way in the systematic nationalization of policing in the 17th century. Nationalization of policing followed throughout the rest of continental Europe and was concentrated largely in towns, which often deferred to the private authority of the landowning aristocracy. In the United States, where cities gradually governmentalized policing in the middle of the 19th century, private policing never really died. The economic boom in the late 1990's increased wages and rates of employment. This impacted the reduction of crime. During the 1990's criminal punishment also increased. Once convicted, prisoners now stayed incarcerated longer. Crime appears to decrease when punishment increases and the reverse proves true as well. In 2017, the need for more prison space has increased and although the cost of building and maintaining more prisons is high, the cost of not doing so appears to be higher. The current economy is forcing the early release of prisoners and the effects have yet to be determined especially in California.

Terence J. Mangan and Michael G. Shanahan have documented the movement in more recent times (1990). While the 1960s was characterized as a period of indifference toward private security, and the 1970s as one of changing perceptions and some mistrust of the industry, they rightly predicted the 1990s would be an era of collaboration and joint ventures between public law enforcement and private security. In the future, this trend will continue. This is necessitated by the fact that individual and corporate citizens who are policed by public law enforcement are also increasingly becoming the clients of private security, as illustrated by the use of corporate security and the increase in the number of gated communities.

The goal for police departments is to continue the reduction in crime rates. However, achieving this requires more policing and more cost precisely when law enforcement agencies

[3] For graphic representations of the trends on expenditures for law enforcement officers and number of police officers compared to private security agents, please visit www.ncpa.org/studies/s181/gif/s181c.gif and www.ncpa.org/studies/s181/gif/s181d.gif

face serious recruitment problems, additional equipment costs, a decrease in tax revenues, and legislative restrictions denying access to any surpluses. “Many municipalities and counties lack the necessary funds due to legislated limits on taxation and spending. Fortunately, privatization of certain police functions has proven a powerful solution to the problem. The steady decline of governments’ capital resources and their increasingly urgent search for ways to continue providing the services that citizens demand without raising taxes are driving the privatization trend. Some federal agencies have saved as much as 50 percent by hiring contractors to provide services” (Smith, 1991). Just as corporations outsource many services to enable them to concentrate on core competencies, the use of private firms by law enforcement agencies frees them to concentrate their efforts on duties that only trained police officers can, and should, do. Public-private partnerships can provide many benefits, especially in terms of pairing law enforcement with a private security provider to save public monies.

Perhaps the most promising but least studied source of external support for police reform is the private business community. Not only do private sector companies command political attention, they hold talent, dynamism, creativity, and a wealth of resources that can be useful to reformers within police agencies. At the same time, partnerships with private businesses, if poorly structured, can erode the professionalism and legitimacy of police organizations. The most successful police leaders who welcome or promote partnerships with the business community are careful not to adopt the profit motive of business as their own, nor to assume that all business people necessarily understand customer service or quality control (Bhanu & Stone, 2004).

Moreover, simply by engaging with police leaders in the process of retraining the front-line staff, business leaders can help build a culture of service in police organizations. As David Bayley notes, “Increasing contacts between police personnel and respectable, non-criminal members of the public is an important way of encouraging the development of an accountable, service-oriented police organization” (Bayley, 2001). The police depend on citizens to assist in almost every aspect of crime prevention and investigation. Mobilizing that public support is essential to the core mission and good treatment of the public is one way to build public

support. Good treatment and professional service are hard enough to deliver in calm encounters between police and citizens, but particularly challenging in the emotionally charged circumstances in which citizens and the police typically turn to each other for help. “Apart from officials in specialized crime detection agencies, most operational police officials engaged in routine, day to day, policing probably spend most of their time assisting people who are experiencing some kind of personal emergency” (Crawshaw, Devlin, & Williamson, 1998). Like the most successful businesses, police organizations should be recruiting, training, and supervising to achieve the highest level of service to citizens.

Examples of Private/Public Partnerships

Lakewood, Colorado

Lakewood offers an example of the benefits of outsourcing law enforcement tasks to private firms. Lakewood has a population of 154,000 within the metropolitan Denver area. Its progressive approach to public-private partnerships in law enforcement is demonstrated by its track record. The city has contracted with outside firms for police department assistance for over 25 years. This progressive attitude comes from a community known for its quality policing — due to its recruitment and training programs, and its 48-year history of requiring college degrees from its officers. Lakewood has produced more police chiefs per capita than any other city in the nation. Approximately one of every ten officers hired in Lakewood has gone on to become top law enforcement executives. They include the chiefs of departments in Naperville, Illinois; Clearwater, Florida; Kettering, Ohio; and the recent International Association of Chiefs of Police president, Plano, Texas Chief of Police, and City Manager.

The Lakewood Police Department was recognized in 1996 as one of the eight best suburban law enforcement police agencies by a panel of experts queried by Good Housekeeping magazine. It is a two-time honoree by the Colorado Association of Chiefs of Police for innovation in law enforcement. In 2002 Lakewood received the Pioneer Award for its public/private partnerships with FirstWatch Security, which was also responsible for security at

the Denver International Airport. As of January 1, 2011, a new agreement was established with G4S Secure Solutions U.S.A. (formerly Wackenhut). Currently they pay $45.00 per hour for Crime Scene Security (12 hour minimum) and Hospital Prisoner Security (4 hour minimum) and $60.00 an hour (12 hour shift) for a marked vehicle.

Many crime scenes take an average of two days to process. Since 24-hour protection is required, it makes complete economic sense to utilize private security for this assignment at a much lesser cost. The G4S officers are specially selected for crime scene detail based on their background and experience, and often attend Lakewood Police Department roll calls for training (just as members of the Lakewood police attend G4S roll calls). The G4S officers know the rules of evidence, and many are certified police officers in the state of Colorado. They provide 24-hour assistance, typically responding within four hours of the department's request. All have been investigated for background clearances and have been processed through the Colorado Bureau of Investigation to ensure they have no criminal record. As Russell Ruffin, a reporter for Law Enforcement Television Network puts it so succinctly, "Paying a private security officer an hourly rate to guard a prisoner or a crime scene frees up police officers. Police don't have to call in an officer on overtime or pull someone off patrol duty" (Ruffin, http://www.ncpa.org).

New Orleans, Louisiana

During the wake of Hurricane Katrina, an investigative report condemned the New Orleans Police Department on virtually every aspect of police work. Although many NOPD officers should be praised for their actions, their stories will likely never get told because of the callous disregard for the truth displayed by some members of the department. Trust is the glue of policing, and success is improved when there is a partnership in keeping communities safer. Police can help develop a symbiotic 'we' relationship instead of an 'us and them' one by making transparency and approachable visibility part of their equation in 'protecting and serving.'

Currently, the NOPD is under a Department of Justice consent decree. The DOJ issued recommendations to improve the NOPD and ensure fundamental cultural change. The goal of the DOJ recommendations is to spark reforms that will take hold and remain in place more than a decade from now. The recommendations include a significant emphasis in transparency, community engagement, and sustainability. Twenty community leaders from industry, academia, and the clergy serve on the board of The New Orleans Police Foundation, a public-private partnership dedicated to strengthening the police department and promoting public safety in New Orleans. Leaving police oversight to other agencies, the foundation focuses on crime reduction. Since its creation in 1995, the Foundation has changed the police department's definition of 'success' from number of arrests made to reduction in crime rates. It has sustained the interest of the business community by showing the correlation between the drop in crime rate and rise in hotel room occupancy. It provides material support to police officers by way of health insurance and tuition reimbursement. The Foundation maintains open communications with the mayor's office, city council, federal agencies, and the police department.

Fresno, California

In just one example, one can see the savings which were reaped by the Fresno, California sheriff's department by outsourcing its transport of prisoners. It cost the department $284 to transport a prisoner from San Diego to Fresno using a private firm. The same trip using sheriff's department personnel and equipment would cost three times as much (West, 1993).

San Francisco, California

Like many police departments around the country, the San Francisco Police Department was slow to adopt cutting-edge technology—no surprise considering the chronic lack of funding for law enforcement. Hundreds of cities rely on COPLINK, a system for sharing information among multiple jurisdictions, but few go to the trouble of building their own data warehouse. In

fact, SFPD until recently was practically devoid of technology—ironic considering San Francisco's standing as a technology hub. Crime reporting methods in the city by the bay had not evolved for a long period of time. The police department did not even have department-wide e-mail until 2011. SFPD has quickly shed its Luddite past. The web-based crime data warehouse is operational (containing over two decades of text, photos, maps, sound, and video), and the department has rolled out an app designed to let officers file reports and access the crime data warehouse with tablets and smartphones. Former Police Chief Greg Suhr wanted to allow officers to stay in the field longer, instead of spending hours in the office filing reports on computers.

San Francisco's embrace of technology followed the arrival of Ed Lee as mayor of San Francisco in January 2011. Appointed by the Board of Supervisors to serve out the term of Gavin Newsom — who had been elected state lieutenant governor — Lee went on to win the mayoral election. Unfortunately, Mayor Lee passed away in 2017. Lee wanted to modernize city government. He came to office with an important ally – Ron Conway, Silicon Valley's current super-angel par excellence. Conway backed Lee in the election and wanted a business-friendly city government. He figured Lee, with some help, could bring San Francisco into the 21st century. After the election, Lee and Conway created San Francisco Citizens Initiative for Technology and Innovation, to "leveraging the collective power of the tech sector as a force for civic action." It now boasts nearly 300 member companies representing 90 percent of the city's tech population. The Citizens Initiative gave $100,000 for development of SFPD's crime data warehouse, as well as the new mobile app. Hewlett-Packard chipped in with 60 high-end notebook PCs, that gave officers in the field access to the crime data warehouse.

The new mobile app, developed by Citizens Initiative member ArcTouch, lets police dispense with the paper, cameras, and audio recorders they have traditionally carried into the field. Instead, officers with tablets or mobile phones use GPS, image recording, and speech recognition to create crime reports in the time it takes to grab a doughnut and a cup of coffee. The reports can be transmitted from a mobile device to the crime data warehouse, where the real-time information can help other department personnel track trends, match suspects, and

generally make the city a safer place. ArcTouch said the app will delivered "the holy grail — any information you need, available at any time." Who would have guessed that the super cop of the future would be armed with an iPad?[4]

Chicago, Illinois

Partnerships between local law enforcement agencies and private businesses are trending, especially in cyber space. The city of Chicago's camera system includes a network of public and private surveillance cameras. About half of the video feeds available to the Chicago police come from private cameras that can be accessed by law enforcement personnel. The Chicago Sun Times reported in a 12/13/2016 article that there are 2700 public safety cameras in Chicago that are part of a broader network of 27,000 private and governed-owned surveillance cameras. Mayor Rahm Emanuel stated in the same article that cameras "have been extremely" helpful in fighting crime particularly on the Chicago Transit Authority. Chicago's Office of Emergency Management and Communications conducts audits to ensure that only approved personnel have access to the surveillance system and use it appropriately.

Public and private sector partnerships between police and private security guards will continue to expand, especially in Chicago where high tech cameras out number police officers. The problem with programs such as Chicago's latest public/private policing strategy is lack of oversight, clear boundaries, and vetting - just to name a few. Private security agencies are regulated by each state. Therefore, hiring standards, training and background checks vary. While the video feed will go to the CPD, the private security firm will have access to the live video feed in the office and in the security patrol cars.[5]

[4] Einstein, D. "San Francisco Cops". Retrieved July 25, 2012 from www.forbes.com.

[5] "Chicago police partner with private security firm". Retrieved June 3rd, 2012 from www.examiner.com.

Minneapolis, Minnesota

In 2003, Target Corporation footed the bill for at least 30 security surveillance cameras it shared with the Minneapolis Police Department. Target's Safe City initiative was an unprecedented merge into the government's business following 9/11. London-style cameras were installed over a 10-block shopping area including Target's corporate headquarters and the Target Center. Civil rights groups argued that the Safe City initiative would impact U.S. citizens' rights to freedom of expression and privacy.

United Kingdom

Even in some of the best resourced and most respected police organizations, business leaders are guiding the process of continuing reform. In the United Kingdom, for example, London First, a membership organization of some of the biggest London businesses, is sponsoring 'joint mentorships' that pair business leaders and police borough commanders to exchange views and expertise. London First is applying business practices in recruiting and training to improve those functions in the police service and plans to use the business community's expertise in marketing and communications to improve the profile of the police in London. Organizers assert that London is already one of the safest cities in the world, but they insist that business leaders have a role in making it even safer and better policed.[6]

How to Approach a Public/Private Partnership

To take advantage of the many benefits a public/private partnership can provide, especially in terms of pairing law enforcement with a private security provider to save public monies, keep in mind the following recommendations issued by the Independent Policy Report (Blackstone & Hakim, 1996):

[6] Partnership in Policing (February, 2001). http://www.c-london.co.uk/data/partnership in_policy.pdf.

- Services that have the potential to be priced should be considered candidates for private provision or user charges.

- Consideration should be given to privatizing tasks that do not require the full range of skills of public police officers. Not only would savings be obtained, but also police officers would become more available for performing the tasks only they can perform.

- Services such as response to alarms could be provided privately. In any case, the owners of alarms should pay for the services they demand. Salt Lake City and Las Vegas have model verified alarm programs.

- Private security can be effective in a distinct geographic area. Therefore, apartment complexes, among others, ought to be encouraged to consider private policing. Competition among apartment complexes to provide safer environments ought to be encouraged. In fact, requiring or encouraging publication of apartments' safety experience might be desirable to permit renters to make informed choices.

- Governments would probably be well served by facilitating an expansion of private security. Any relatively low-skill or specialized high-skill services that are currently provided publicly could be considered as candidates for transfer to private security.

- Monitoring contractor compliance and performance must not be so costly as to eliminate the savings from privatization.

- State legislatures should consider whether the current legal status and regulations pertaining to private security are appropriate in view of the expanded role expected from private security. Specifically, emergency vehicle status and expanded powers of arrest ought to be examined.

- Problem-oriented policing is a method that offers the prospect of improved police/private partnerships in dealing with specific crime problems.

- Governments should be encouraged to expand the use of community policing, because the approach offers hope for improving police performance and the community's sense of participation. Like privatization, community policing helps society better determine the use of its scarce police resources. Further, it brings the police "back" to constituents. Successful community policing satisfies the desires of the community.

Conclusion

The importance of trust and transparency with law enforcement and the community are essential to the success of both entities. It is the duty of every police leader today to embrace

the challenge, understand the complexities, and take bold, proactive, transformative actions that will close the gap between where we are and where we must be. The dialogue is taking place in communities across the United States. If agencies are willing to listen with grace and respect, engage in intellectual honesty and professional introspection, and seek the kind of mind shifts and heart shifts required of twenty-first century policing, then they have the opportunity to truly be guardians of the great democracy.

Reference

Bayley, D. H. (2001). *Democratizing the police abroad: What to do and how to do it*. Washington, DC: U.S. Department of Justice.

Bayley, D. H. & Shearing, C. D. (2001). *The new structure of policing: Description, conceptualization, and research agenda*. Washington, DC: U.S. Department of Justice, National Institute of Justice.

Bhanu, C. & Stone, C. (2004). *Public-private partnerships for police reform*. New York: Vera Institute of Justice.

Blackstone, E. A. & Hakim, S. (1996). *Police services: The private challenge*. Oakland, CA: Independent Institute.

Crawshaw, R., Devlin, B. & Williamson, T. (1998). *Human rights and policing standards for good behaviour and a strategy for change.* The Hague: Kluwer Law International.

Mangan, T. J. & Shanahan, M. G. (1990). Public law enforcement/private security: A new partnership? *FBI Law Enforcement Bulletin*, 59(1), 18-22.

Reaves, B. (2006). *Census of state and local law enforcement agencies, 2008*. Washington, DC: Bureau of Justice Statistics.

Smith, W.J. (1991). Private sector development: A winning strategy for new police stations, sheriff's stations, and jails. *The Police Chief, 63*(8), 29-33.

West, M. L. (1993). Get a piece of the privatization pie: Private security agencies. *Security Management*, *37*(3), 54.

The Friday Crab Club, Redux

Joseph A. Schafer

August Vollmer stands as a giant in the history of police professionalism in America. As leader of the Berkeley (CA) Police Department from 1905-1932, Vollmer worked tirelessly to advance the image that policing was not simply a job, but was a profession. As such, officers were expected to be educated, articulate experts who could use contemporary technology and knowledge to deliver policing services with integrity and quality. Vollmer played a major role in advancing higher education in policing, contributing the emergence of criminology and criminal justice as legitimate academic disciplines. He emphasized problem solving, analysis, and the empowerment of front-line personnel. Though Vollmer's vision of professionalism and education may differ from the ideals we pursue a century later, his legacy endures. Though history tends to emphasize his role as an advocate for education, Vollmer was also innovative in how he thought about organizational practices and employee relations.

As an iconic figure, much lore surrounds the way in which Vollmer led his own agency. It is quite possible his legacy has become romanticized, yet even if they are not entirely accurate the accounts of his approaches in Berkeley are instructive because of what can be learned about models for organizations and personnel management. Among other approaches Vollmer utilized in Berkeley PD was the Friday Crab Club. Based on archival research and interviews with former Berkeley officers, noted Vollmer biographers Gene and Elaine Carte described these meetings as follows.

> Every Friday, all officers not on duty attended a group meeting to discuss department matters. One officer recalled: "If you fired your gun, you would have to get up before the whole group on the Friday Crab Club hour and give the factors on what happened, and there was a decision made by the men from the standpoint of this way or this way; right or wrong. The Friday meetings, informally called the Crab Club, were a combination gripe and learning session. "For instance, if you had anything against any man in the department, you said it right there in front of him, and after it was over it was forgotten, "remembered one officer. (1975, pp. 46-47)

The Crab Club served two important functions. First, it was a venue in which peer review ensured accountability and professionalism. Officers had to answer to their co-workers when they engaged in high consequence actions, such as discharging a firearm. Oversight and accountability were not simply imposed from top executives; they were expected aspects of peer-to-peer relationships. Second, the Crab Club was a venue to resolve interpersonal disputes and conflicts. Problems among co-workers were not allowed to remain hidden, where they might fester and grow; they were to be resolved in a direct and timely manner.

To Vollmer's way of thinking, it was important for officers to have a chance to discuss interpersonal conflict in a suitable manner; bad feelings should not linger and worsen. If two officers had a disagreement, that matter should be aired and resolved quickly. If officers had questions about management practices, they needed to have the chance to voice concerns and seek further information before resentment and resistance could take hold. If an incident had occurred during the week that was not effectively handled, the involved parties needed to discuss what happened and what mistakes were made. Officers needed to be held accountable to their peers for their decisions and actions. In many ways, this practice was a precursor to the contemporary morbidity and mortality meetings often held in medical settings. Such events require doctors in training to explain to their peers how a case was handled and honestly discuss the possibility of errors and oversights. The objective was not to shame or humiliate officers, but rather to create learning moments and to ensure poor choices did not become accepted institutional practice. This approach served the added function of reinforcing that officers had an obligation to remain accountable and professional, and that this obligation extended not only to the organization, but to one's peers, as well.

It is possible the lore surrounding this practice has inflated its actual efficacy within the Berkeley PD. Furthermore, changes in professional practices and civil liability might have rendered some aspects of the approach impractical in modern agencies (i.e., officers discussing the choice to discharge their firearms in a peer-to-peer venue). It is likely police unionism further complicates the contemporary use of the classical model of the Friday Crab Club. Even at the time, it is possible participating officers viewed these meetings not as a chance to air

grievances, but as an uncomfortable experience. The meeting may have been more akin to the hostility and animosity with which some have characterized Compstat meetings in the NYPD in the 1990s (Greene, 1999; Haberfeld, 2006). Historical discussions of these meetings are very limited (Carte & Carte, 1975) and may be of questionable veracity. None of these limitations invalidate the underlying ideas imbued in the Crab Club model, particularly as it relates to the ideas of trust and transparency in contemporary police organizations.

For the purposes of this essay, I would ask the reader's indulgence by sticking with the mythical, if not-fully validated image, of the Friday Crab Club. Consider the idealized image of an institutionalized management practice that created a reasonably safe and neutral environment in which two officers could discuss interpersonal differences, disagreements, and conflicts. While these officers might not become fast friends as a result of the Friday Crab Club, the experience might allow them to prevent their conflicts from growing and impeding their ability to do their job effectively. Consider a venue in which officers could ask questions about policies and procedures, allowing management to receive input and allay concerns. Rather than operational edicts being meet with resistance and obfuscation, they could be understood and (perhaps reluctantly) accepted. Consider a management practice that made accountability not simply something imposed on officers by their superiors, but ensured accountability was something officers understood they owed to their coworkers.

In considering the nexus between the Friday Crab Club and police unionism, Kelling and Kliesmet (1995) suggest Vollmer was ahead of the management thinking of his time.

> In other words, Vollmer, before the management theories of Frederick Taylor became integral to the reform model, was experimenting with the development of a genuinely professional model of policing. This model included higher education, collegial control, a generalist police practitioner, specialties at the service of generalists, devolution of authority to practitioners, and collaboration with other professions (p. 200).

Imagine the existence of a forum in which officers and organizations learned from mistakes, rather than seeking to bury errors and/or vilify those deemed (rightly or wrongly) to be at fault. Police officers and agencies could become learning organizations (Geller, 1997) by turning past

problems into teachable moments. The Friday Crab Club created a forum in which officers could exert collegial peer-to-peer accountability to, and control over, one another, rather than relying on a chief to exert complete command and control upon front line personnel and their professionalism. Control in the work place was done *with* one's co-workers, rather than being a force *imposed upon* one from on high.

Whether the Friday Crab Club truly worked in this purported fashion or has simply become romanticized over time is largely immaterial. What is helpful for these purposes is the power of the image rather than the veracity of the claim. What such a Crab Club would provide is a safe forum in which 'dirty laundry,' ill will, and mistakes could be aired in a safe manner. Officers might not like all their peers. Officers might not like every management decision. The agency might not agree with every decision made by its officers. The Friday Crab Club would not have created a completely harmonious and friendly agency. The idealized notion conveyed by the example, however, is of an agency that addresses potentially toxic matters in the healthiest way possible. The Friday Crab Club would be a well-regulated septic system. Fecal matter is still produced, but it is handled in the safest and most sanitary way possible; properly functioning, undesirable by-products still exist, but they are contained and don't spill over into areas they do not belong. Internally, it might be expected that trust and transparency would be quite high.

The efficacy of the Crab Club is a powerful and alluring organizational tool that could be beneficial in myriad professional contexts far beyond just policing. One issue that made the idealized Crab Club so intriguing is that it was an internal and private mechanism for matters to be processed, addressed, and resolved. Though perhaps not all participants were or would be completely satisfied with the process and outcome, the idea conveys a vision of organizations dealing with internal strife and conflict in a constructive manner. Ideas would be allowed to flourish, enjoy refinement, and benefit all involved. The choices of executives and supervisors might be explained to followers. In effect, the 'dirty laundry' of the organization might be aired in a safe, private, and healthy manner, while also advancing innovation and employee-initiated efforts in the workplace.

Friday Crab Club, Redux

Few organizations of any type likely meet the idealized vision of the Friday Crab Club. Conflict is allowed to fester. New ideas are not encouraged. Communication flows up the organization, while those at the top often do not do enough to provide information to those they lead. The police, like so many other organizations, suffer from unhealthy internal communication and conflict management. In past eras this situation left few options for affected personnel. Officers were left to vent to one another in small groups while huddled around water coolers, meeting in coffee shops, or sitting in idling patrol cars. In rare circumstances, shift supervisors might allow such events to occur during pre-shift briefings. In the absence of a formal Friday Crab Club, officers could express their frustration to their peers. Agency supervisors and executives, however, had no way to receive input or complaints from personnel, perhaps by very conscious design. Accountability remained a force largely imposed upon officers from on high within the organization (though certainly myriad *ad hoc* exceptions to this observation have existed). Co-workers who had a conflict with one another did not enjoy an established framework within which to express their concerns and frustrations. In effect, much of the benefit of the Friday Crab Club was denied to personnel and there was no way for them to compensate for that shortcoming.

The rise of the Internet has redefined the capacity of officers to vent, deal with conflict, and express displeasure with agency leaders, particularly since the early 2000s. A wide range of discussion boards, listservs, blogs, and websites have emerged that allow officers to air grievances (real or perceived), complain, and share concerns with one another.[7] From an organizational perspective this is a challenging evolution. Two officers venting about the chief while drinking coffee in a donut shop might actually be a healthy process. Those same officers having the same exchange in a public online forum opens the conversation to the entire world and creates a record of that conversation that, if not permanent, is at least long-lasting. Morale

[7] Examples of this situation abound, though they tend to be transitory in nature. Among other examples is the website leoaffairs.com, started by two officers in the Tampa (FL) area and now hosting forums covering agencies from coast-to-coast. These forums were largely a public and anonymous venue for complaining about agencies, leaders, personnel, and practices. Countless blogs and websites have come and gone, creating (at least temporarily) a public Crab Club for a specific agency and/or issue.

can be enhanced through donut shop conversations; morale can be eroded through online discussions.

In the absence of effective organizational practices that allow officers to deal with conflict and disagreement, while simultaneously advancing communication, officers have innovated and created online mechanisms to fill that need. Some of these mechanisms are private or at least restricted to vetted members of the law enforcement community. Others are, by intent and design, completely public and seek to reach community residents, the media, and local political officials. The problem with informal technology-enabled alternatives to the Friday Crab Club is that such innovative alternatives may be public and enduring. They provide external transparency that might ultimately be counterproductive, potentially eroding external trust, and they do not actually provide the full range of benefits presumed under the Friday Crab Club model. The Friday Crab Club, Redux model is driven by technology that makes conflict and disputes matters of public record. They risk making allegations anonymous (perhaps elevating the risk of distortions, half-truths, and blatant lies) and lean toward one-way conversations (i.e., an officer or officers complaining about the agency and/or its leaders, without the benefit of a response from the targeted party). The Redux model is decidedly inferior to the original model because it fails to provide the healthy aspect of the original model…two-way communication and dialog.

The point of the Friday Crab Club, Redux model is that what was formerly hidden (at least in the short term and to the general benefit of the organization) is now quite public. Members of the public are privy to information that was previously unavaible. In some instances and from some perspectives this is a positive evolution. If there are fundamental problems with agency leaders, operations, and decisions it is a boon for citizens and community leaders to know about that situation. The problem, of course, is that not everything expressed in the Redux model is accurate or even a legitimate problem. The Redux model tends to only broadcast the perspective and concerns of those upset with a situation; the official position of the agency and its leaders is almost never transmitted through the same modalities. Thus, the Redux model can be a lone officer speaking truth to power. It is just as likely to be a disaffected

employee or set of employees who are distorting, maligning, and besmirching. It is not a process that facilitates two-way dialog and the resolution of conflict. Rather, it is a process that inflames already tense relations within an organization and exposes a broader to a controversial situation.

Messengers can and do have their own agendas. Conflicts can be legitimized under the gloss of whistle-blowing and 'speaking truth to power.' Lies and innuendo can be leveraged against those the messenger dislikes for any number of reasons. Every organization, as every family, has problems, conflicts, and skeletons in the closet. Revealing even true concerns with complete transparency can make it more difficult to correct and resolve problems. It is not always beneficial for children to know their parents are experiencing marital strife. Such awareness can sometimes complicate or impede the ability to correct the problem. Parallels exist with the problems police organizations confront. The public does not always benefit from knowing aspects of an executive's personal life or that the sheriff has just promoted her nephew within the organization. Sometimes what appears to be nepotism is blatant favoritism; other times the nephew might be the best person for the promotion.

A chief once related to the author that upon assuming command of a large agency he learned of an officer who operated a blog that was widely read by agency critics and the local media. The blog assailed a number of problems in the agency and among its executives. The officer did not openly disclose his identity on the blog, but everyone in the agency knew who was writing the blog. The chief expressed that the officer's actions, while well intentioned, were misdirected. The officer sought to shed light on persistent problems in the agency; the officer presumably saw himself as a whistle-blower who was seeking to advance the organization in the long-term. From the perspective of the chief, however, the officer was actually making it more difficult to address persistent problems in the organization, particularly as an outsider assuming a new command. The blog reduced morale among many in the agency. It sowed the seeds of discontent. It provided 'ammunition' to agency critics throughout the city. It made the agency appear inept rather than normal. Every large agency has problems and no employee will agree with all decisions made by their leaders. Rather than serving to heal wounds, the blog

aggravated old wounds and inflamed new problems. Even if the officer was generally right, the actions inflicted further damage on the organization.

From the viewpoint of officers engaging in the Friday Crab Club, Redux model, however, what alternative do they have? Their agency provides them with no acceptable way to express concerns, ask questions, and deal with conflict. The ease and visibility of the Redux approach is seductive. Though it brings the wrong transparency to the organization, at least it provides transparency that otherwise might not exist. To make a broad generalization, the Redux approach is not likely to emerge in healthy and functional organizations. As a graduate student, the author took several courses in labor relations taught by an elder statesman of the union movement in America. He repeatedly remarked that unions rarely emerge in organizations that have healthy labor-management relations. If employees are content in the workplace they have little reason to seek to organize. Parallels might be seen to the use of modern technology to facilitate the public airing of what was private in the classical Friday Crab Club model developed and employed by Vollmer. The Redux model is a move of desperation by those who feel they have no other way for their voice to be heard. Clearly there might occasionally be a problematic employee in even the best organization. Yet on the whole, we would not expect to see the Redux model emerge when employees are content with existing structures and mechanisms.

The Nexus with Trust & Transparency

The opening chapter of this volume presented the idea that trust and transparency exist on two dimensions in policing: internal and external. Though perhaps not explicit or intentional, the traditional Friday Crab Club model generated needed internal trust and transparency. Officers were held accountable, disputes could be resolved, and management interacted with line personnel to exchange ideas, field questions, and address concerns. Yet the proverbial dirty laundry within these processes was aired away from public view. In this way, Vollmer could generate strong internal trust and transparency. Because matters were resolved in house there was little fodder to fuel media scrutiny or local concern with police operations. In this way the Friday Crab Club model helped generate external trust and transparency by minimizing public

evidence that citizens had a need to be concerned with the Berkeley Police Department.[8] Healthy internal operations are likely to engender healthy external relations. When top agency leaders seek to address internal strife, conflict, and controversy in a healthy, direct, and functional manner, it might be expected that orientation will (more often than not) extend outward to the ways trust and transparency are nurtured and maintained with the community and other external parties.

The ease with which officers can implement the Redux model amplifies the importance of modern leaders attending to internal trust and transparency. Unlike prior eras of technology, officers do not have to suffer in silence within the workplace. Someone upset and discontent with aspects of their organization has an all-too-easy way to vent that situation not simply to a co-worker over coffee, but to the entire world (perhaps even while on-duty using a smartphone or tablet). Leaders cannot completely circumvent the prospects that officers will use the Redux model, no matter how healthy the internal aspects of the organization. But leaders cannot pretend or presume they can prevent the use of Redux model approaches. The transparency found throughout the contemporary world will only continue to expand and grow. The rise of Redux approaches should reinforce that wise leaders will study and consider how they might facilitate a healthy and functional revitalization of the Friday Crab Club. Technology has made the Redux model a weapon used against agencies and leaders. This does not have to be the case. Technology can be use to reinvigorate and reinterpret the classical Friday Crab Club model in a way that, while not perfect (and it certainly was not perfect in BPD 100 years ago), can lead to greater internal trust and transparency in the workplace.

[8] To be sure, this does not suggest that citizens would be accurate in viewing BPD (or any other agency handling internal disputes in a private manner) as trustworthy and transparent. The absence of smoke does not always mean there is an absence of fire. It might be expected that suppressing public awareness of officer/organizational misdeeds is a temporary fix. Over time, it would be expected that efforts to preserve public trust by decreasing external transparency will fail and perhaps have worse consequences for the agency and its executives.

References

Carte, G.E., & Carte, E.H. (1975). *Police reform in the United States: The era of August Vollmer, 1905- 1932*. Berkeley, CA: University of California Press.

Geller, W.A. (1997). Suppose we were really serious about police departments becoming 'learning organizations?' *National Institute of Justice Journal, 234*, 2-8.

Greene, J.A. (1999). Zero tolerance: Police policies and practices in New York City. *Crime & Delinquency*, 45, 171-187.

Haberfeld, M.R. (2006). *Police leadership*. Upper Saddle River, NJ: Pearson-Prentice Hall.

Kelling, G.L., & Kliesmet, R.B. (1995). Police unions, police culture, the Friday Crab Club, and police abuse of force. In W.A. Geller & H. Toch (Eds.) *And justice for all: Understanding & controlling police abuse of force* (pp. 197-204). Washington, DC: Police Executive Research Forum.

Fostering External Trust and Transparency through the Use of Police Agency Websites

Michele W. Covington and Nicholas E. Libby

Introduction

Since its inception in the United States, one of the inherent problems in policing has been the lack of trust between agencies and the communities they serve. Trust and oversight were principal issues for many years. This was especially true before the age of professionalism, when agencies began to clean up their misconduct, cut political ties and focus on policing as an independent profession. The lawlessness of the police, their systematic corruption, and nonenforcement and selective enforcement of the laws was one of the paramount issues in municipal politics during the late 1800s (Uchida, 2010). Historically, the tenuous relationship between officer and constituent has caused many problems, but in recent years, with increased concern over ethics and transparency and with the dawn of the community policing era, this stress and mistrust has come to light and started to decline. Between the recent popularity of community-oriented policing strategies and a more fervent public demand for honest and trustworthy police agencies, methods to increase external transparency have become major topics of debate for agencies today. Trust and transparency in policing are not optional; they are mandatory for police agencies in any society that wish to demonstrate legitimacy (Markham and Punch 2007, 300). Fostering trust and transparency is an especially important topic in the current era given the rise of 24/7 news networks and proliferation of personal accounts and experiences that may be readily accessible online in both text and video formats, even though both news and personal accounts may have questionable accuracy or simply not be developed enough to tell the entire story. While there has been a wide range of the level of openness based on agency location, size, and leadership, there has been a recent general shift in attitude that has led many agencies to be more open with their information and to want to communicate with the public directly.

Along the same timelines as the attitudinal shift to more open agencies, there has been an upswing in societal uses of technology. Within recent years, we have witnessed a massive proliferation of personal computers, tablets, and smartphones alongside increases in availability of publicly accessible broadband wireless internet access and home internet use. According to the US Census Bureau (File & Ryan, 2014), as of 2013, 74.4% of households reported having an internet connection in the home, a trend which has been increasing steadily since the late 1990s (File, 2013).

This rise in the use of technology has completely altered the American way of communication. For example, the proliferation of cell phones has made it possible for most people to get in touch with nearly everyone they know, no matter where they are. Furthermore, increases in the availability of wireless networks, tablets, and smartphones has made it possible for people to gather information online even when away from their home and office computers. Relatively recent advances in communication, such as e-mail, have begun to be overshadowed with the advent of social networking sites and the ability to send text messages rather than make phone calls. With the recent exponential increase in capability and affordability of technology, many police agencies with the resources to spare have found little reason not to move along with the technological revolution. This is a proactive approach for agencies to take. Using the internet, specifically agency websites, to voluntarily provide information to the public shows goodwill and portrays the police agency as more transparent to the outside world, especially to the community it serves.

The recent movements toward more transparent police agencies and more widespread use of technology are still going strong, and there is no indication that either of these trends will slow down in the near future. Considering this, many agencies are now exploring different options to openly share information with the public. One way for agencies to accomplish this goal has been the development and use of individual police agency websites, which have become very common over the last few years. One-hundred percent of the largest agencies in the U.S. and over 40% of all agencies use an agency website to some extent (Kilburn & Krieger, 2014; Rosenbaum, et al., 2011). These sites can be tailored to any agency's specific need, and

almost any agency's budget. There are many options for external information sharing through an agency website and many advantages to so doing.

Strategies for External Communication

Information gathering on police agency websites is bidirectional: citizens can go online to *receive* information from a police agency or to *provide* information to the agency. Many police agencies, such as the New York City Police Department (www.nyc.gov/html/nypd/) and the Orlando Police Department (www.cityoforlando.net/police) have designed their websites to be able to receive information from the public, such as crime tips or service requests that do not necessarily require one-on-one interaction. This frees up personnel resources and may make citizens more comfortable providing tips or other information if they feel a greater degree of anonymity and do not have to face an officer or other police employee in person. It may lead citizens to feel that they are more invested in their communities and that they enjoy more of a working relationship with their local police agency rather than feeling ingrained in the traditional 'us vs. them' mentality.

Using an agency website to *collect* information from citizens can benefit an agency, but agency websites are most helpful in *providing* information. Recently, more and more agencies have begun to use their websites as a direct line of communication with the public. Historically, the main outlet of information about local police has been local media, which was not always an ideal situation. The quality of relationships between police agencies and media outlets varies widely from jurisdiction to jurisdiction, and there have often been problems when a story was reported in a biased manner or when the local news agency ran a story without all of the pertinent information. Problems stemming from media coverage of police stories have led agencies to find their own means of communicating with the public; in the information age this has meant rapidly increasing the use of websites.

Furthermore, in many areas the types of information provided to the public by internet is far broader than in the past when websites simply showed a picture of the chief, the agency's

address, and a phone number to call to become an officer. Agencies now provide such a wide array of information through their websites, such as crime maps (Louisville (KY) Metro Police www.louisvilleky.gov/MetroPolice/) and maps of calls for service (Colorado Springs (CO) Police www.springsgov.com/police), links to current agency initiatives (Phoenix (AZ) Police http://phoenix.gov/police), and even selected information from incident reports (Madison (WI) Police www.cityofmadison.com/incidentReports). Police agency websites are now used to publicize most wanted suspects (Roanoke (VA) Police www.roanokeva.gov › Departments and Divisions › Police), missing persons (Fort Smith (AR) Police www.fortsmithpd.org), and to provide links to websites for sex offender registries and other pertinent law enforcement agencies (Metropolitan Police (Washington, DC) http://mpdc.dc.gov).

In addition to crime maps and incident reports, agencies can make their own recordings of events such as news interviews with police officials and meetings between police officials and the general public and post these on agency websites. Not only does this broaden the scope of information available to the public, but it can also serve as a record of police interaction that is unedited by a third party, such as the news media. To further foster public and police interaction, many agencies have made use of social networking websites such as Facebook and Twitter to provide information to the public or receive feedback from their constituents. In some cases, this route can be beneficial to smaller law enforcement agencies that do not have the resources to host and maintain their own website.

Advantages of Website Communication

The types of information provided by police websites have increased significantly in recent years and by all indications they will continue to do so in the future. In large part, this is because there are significant advantages to this method of direct communication with the public. In terms of external trust and transparency alone, the internet is an excellent route of communication. Many Americans now go online to search for almost any information they need and it behooves agencies to be a source of that information. When a citizen goes online and types the name of their local police agency into a search engine, a video of a fight between

an officer and a citizen on YouTube does not have to be the only source of information; this is an excellent opportunity for citizens to find a link to a story on the agency website about a recent successful drug raid that made the community a safer place. So often the public only sees the negative aspects of police work and examples of broken trust between officers and their communities. Agency websites can provide an outlet where good news can be shared, as well.

Using a website to disseminate information can save agency resources because a user-friendly website can prevent an employee from having to answer so many inquiries personally. A survey of 1,379 police agencies serving a population of 25,000 or more, found that almost three out of four chiefs received statistics requests at least monthly (JRSA, 2005). Almost one in three received these requests at least weekly. Requests for simple statistics and more could be handled through a website in which the public could retrieve the desired information themselves. This would require relatively little maintenance when up and running and the agency would have full authority over what types of information to release. Obviously, disseminating information on demand through a website is more likely to be cost effective for larger agencies serving larger populations, but there are some benefits that apply regardless of agency size. Any time an agency willingly puts information out for open public consumption, it reflects goodwill on that agency. The agency appears open and willing to share with the public and establishes a direct line of communication by using a medium through which many citizens enjoy communicating.

Challenges of Website Communication

Of course, there are inherent dangers in sharing information with the public via website, some more problematic than others. Obviously, police agencies must carefully control the data that they release to the public for tactical and safety reasons, as well as for ethical and legal concerns. Someone must approve what information is released and what is to be held privately. With these decisions, it is important not to choose information to release based on biases toward the agency. Agencies must not use their websites as false transparency to garner

goodwill from the public when they are actually releasing biased information; this will only lead to *mis*trust between the agency and the public. Along the same lines of choosing which data to release, there is always a risk that the information will be misinterpreted. It is crucial to keep the information simple and easy to understand and to provide explanations and definitions wherever appropriate. Furthermore, there is often a time lag in the data displayed on the website because of the time it takes to get the data put into the system and onto the site after it has been approved for release. It is important to avoid confusion by clearing stating how far behind the current date the information is and to provide a brief explanation for the gap in layman's terms.

Data may have inaccuracies; it is of utmost importance to ensure the quality of the information released as much as possible. In a large agency releasing large amounts of information through the web, some errors are likely. Even agencies with conscientious employees who double check the data being released will probably find an occasional minor error. This may cause ethical problems if incorrect information is released, but it could also lead to legal problems. It may be beneficial for agencies to consult a legal authority about their responsibilities and about the option of including on the website a disclaimer against errors made in good faith.

Another challenge for an agency that wishes to communicate through a website may be cost. Although having a website set up is relatively inexpensive now, many agencies are struggling in the current economy to find funds in the budget to remain staffed, much less to expand the technology under use. For larger agencies, using a website for information sharing will be cost effective as this will free up manpower to be used elsewhere rather than responding to calls for information, service, or complaints. Smaller agencies, however, may not receive as many requests for information. It may still behoove smaller agencies to have a website for exposure, but agencies that serve smaller populations (and usually have smaller budgets) may choose to offer less features on a website than larger agencies, allowing for very little maintenance once the site is up and running. This can provide basic information for the public through a medium that many citizens now prefer to use with almost no cost after the

initial setup of the site. Furthermore, as mentioned previously, agencies can also opt to take advantage of free services provided by social networking websites such as Facebook and Twitter in order to maintain an online presence with the public or to supplement their existing website.

A final potential issue to consider is that while internet use is quite high in the United States, it is not a method of communication that every person uses. The use of a website to share information and increase transparency will reach many citizens, but not all of them. Agencies that choose to use this mode of communication should keep in mind that a website is an *addition* to other sources of public communication; it is not a base strategy.

Conclusions

The recent push toward more accountability and transparency between police agencies and the public has led many agencies to look for new and innovative ways to share information and be open with the citizens in their jurisdictions. One method of communication that many agencies have chosen is the agency website. While there may be some areas of concern regarding sharing information publicly through a website, careful planning and decision-making about the information to be shared can eliminate most of these potential problems. At present, however, research has found that easily-accessible websites do influence public perception in a positive way (Kilburn & Krieger, 2014). This strategy seems to be working well for agencies, and the internet savvy public appears to enjoy communicating in this fashion.

As agencies garner more and more data through the use of new technologies such as crime mapping and analysis tools, there is much more information to be shared, and much of it can be very useful to the public. Information that is chosen carefully so as not to compromise security, confidentiality, or the mission of the job, can be shared relatively easily and inexpensively through websites, often saving agency funds while simultaneously fostering goodwill and trust among law enforcement agencies and their constituencies. With the rapid growth in technology in recent years and the push toward more accountability among police

agencies, it may soon be all but required that use of agency websites be part of the toolkit used by police in their interactions with the public. Unfortunately, recent research suggests that many agencies with websites underutilize them (Rosenbaum, et al., 2011), indicating a lack of foresight and proactivity in keeping up with existing and emerging social trends within the general public.

References

File, T. (2013). *Computer and internet use in the United States: Population characteristics*. Washington, DC: U.S. Census Bureau, U.S. Department of Commerce.

File, T., & Ryan, C. (2014). *Computer and internet access in the United States: 2013. American community survey reports*. Washington, DC: U.S. Census Bureau, U.S. Department of Commerce.

Justice Research and Statistics Association. (2005). *Use of data in police departments: A survey of police chiefs and data analysts.* Washington, DC: JRSA.

Kilburn, M., & Krieger, L. (2014). Policing in an information age: The prevalence of state and local law enforcement agencies utilising the World Wide Web to connect to the community. *International Journal of Police Science & Management, 16*(3), 221-227.

Markham, G., & Punch, M. (2007). Embracing accountability: The way forward—part one. *Policing: A Journal of Policy and Practice, 1*(3), 300-308.

Rosenbaum, D.P., Graziano, L.M., Stephens, C.D., & Schuck, A.M. (2011). Understanding community policing and legitimacy-seeking behavior in virtual reality: A national study of municipal police websites. *Police Quarterly, 14*(1), 25-47.

Uchida, C.D. (2010). The development of the American police: An historical overview. In R.G. Dunham and G.P. Alpert (eds.) *Critical issues in policing: Contemporary readings (5th ed.)* (pp. 17-36). Long Grove, IL: Waveland.

Social Media: Use, Policy and Guidelines

Toby M. Finnie

The proliferation of new and emerging social networking technologies presents significant challenges for police administrators and managers. With each technological breakthrough, administrators should forestall use and practices that may reflect negatively upon the department and its employees. Use policies should be written only after drafters gain a basic understanding of how the social media application works, and a risk assessment is conducted.

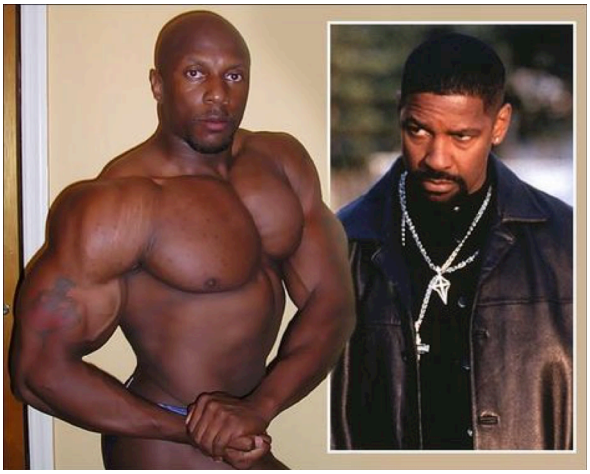
One could not, for example, draft use policy for a telephone without first understanding its operation:

- Lift the headset from the cradle
- Listen for a "dial tone"
- Enter an access code (by dial or by pushbutton)
- Listen for a "handshake" (ringing tone)
- Wait for a response from the party called
- Initiate and complete the conversation
- Disconnect the "handshake" by returning the handset to the cradle.

Terms of use to mitigate risks and liability might require that officers and staff make and receive no personal calls, limit long distance calls, refuse collect calls, and log all incoming and outgoing calls. Officers might also be reminded to maintain a professional demeanor during all telephone conversations.

Failure to analyze emerging technologies, to evaluate for possible use or abuse by personnel, and to prepare use guidelines for both on- and off-duty personnel may lead to unintended and potentially costly outcomes:

- A police department in the Pacific Northwest issued cellular telephones to its officers with no guidelines for use. Administrators were stunned to learn that — a mere 30 days after issuance — officers had exceeded the department's contracted usage allowance *for the entire year!*
- Three police officers were suspended without pay and ordered to undergo sensitivity training after they discussed policing duties and posted offensive remarks about homosexuals and developmentally disabled persons on a Myspace.com web site. (Associated Press, 2006)[9]
- A criminal defense attorney successfully used an officer's comments posted on a social networking web site to infer to the jury that the officer used excessive force during arrest of the suspect. During testimony, the jury learned that the officer had set his MySpace.com mood to "devious" and had posted "Vaughan is watching *Training Day* to brush up on proper police procedure" on his Facebook homepage on the same day he arrested the suspect. The officer also wrote, "If he wanted to tune him up some, he should have delayed cuffing him" and "if you're going to hit a cuffed suspect, at least get your money's worth 'cause now he's going to get disciplined…." (Dwyer, 2009)[10]



An officer's photo images and comments posted on his social media web site came back to haunt him during trial testimony.

Photograph Source: http://www.smh.com.au/articles/2009/03/13/1236447441188.htmll

The officer had uploaded images of himself in bodybuilding poses that could be construed as "intimidating." That

[9] Associated Press (2006, July 7) Police suspended over MySpace comments. KXNet.com North Dakota News. Retrieved October 22, 2009 from <http://www.kxnet.com/custom404.asp?404;http://www.kxnet.com/t/drunken-driving/20905.asp>
[10] Dwyer, Jim. (2009, March 10) The Officer Who Posted Too Much on MySpace. New York Times. Retrieved October 21, 2009 from <http://www.nytimes.com/2009/03/11/nyregion/11about.html?_r=3>

image aided the defendant and jury to positively identify the officer as the owner of the website. The jury acquitted the accused.

In the situations described above, unnecessary expense, negative publicity, and an undesirable outcome at trial could have been avoided had police managers proactively worked to develop guidelines advising officers and staff on acceptable uses of new technology. Consistency in enforcement of clearly written social media use policies will help to protect the agency against liability and reduce employee' misunderstandings about expectations of privacy.

"We are all PIOs now"

The days of department-authorized Public Information Officers funneling the flow of information to media and the public are over. Wise police administrators understand that now any officer or staff member is a PIO, for better or for worse. It should be remembered that news reporters and journalists regularly conduct online searches for background information on police officers, suspects, and witnesses — and so do ordinary citizens, criminals, and defense attorneys. In the past, newspaper and magazine articles tended to become lost in dusty old library stacks, but that is no longer the case. Information posted on the Internet often remains accessible long after a user takes active steps to delete data and images they previously uploaded. Despite popular belief, websites that restrict access to users through log-in pass codes may not provide sufficient barriers to public scrutiny.

In July 2009 three organizations (National Association of Black Law Enforcement Officer, local chapter of the National Black Police Association and NAACP) filed a class action lawsuit in federal court against the Philadelphia Police Department for allowing its officers to post "blatantly racist… and offensive" content on a popular web site devoted to public safety. Also named as a defendant was "McQ," an alias allegedly belonging to a sergeant with Philadelphia police and administrator-moderator of the website "Domelights.com." The lawsuit requested the court to remedy:

"…invidious racial discrimination on the part of the Philadelphia Police

> Department, in allowing, through custom, practice and policy, a group of white Philadelphia Police Officers, including officers of supervisory rank, to operate, publish, disseminate and perpetuate during their employment as police officers, both on and off duty, a blatantly racist, anti-minority, disgusting and offensive public Internet website called Domelights.com that has become an insult to all African-American Police Officers, and has created a racially harassing and hostile work environment…." (Guardian Civic League, Inc. 2009)[11]

The lawsuit alleged the Philadelphia Police Department "…evidenced a policy, practice or custom of allowing the use of their computers for a racially hostile purpose, and allowing its employee Police Officers to engage publically [sic] in racially offensive and hostile commentary and postings" (Guardian Civic League, Inc. 2009).[12]

According to some legal analysts, a successful outcome to the lawsuit would hinge on whether the Philadelphia Police Department implicitly permitted its officers to post comments via city-owned computers, or whether command staff were aware of and disregarded information that officers were posting racially offensive comments while on duty. After the lawsuit was filed, additional risk management problems became apparent: once identity becomes known, "McQ's" susceptibility to retaliation may directly effect staffing assignments. Also of concern is potential retaliation against other officers:

> …[S]omeone outside the department has expressed an intent to operate a website identifying the Domelights regulars — complete with shifts, station assignments, car numbers and badge numbers — and that the command staff fears escalation and therefore wants to defuse this situation. (Post, 2009)[13]

Not only does the loss of trust disrupt police department operations, mistrust and racial biases may flow — like a mini tsunami — into the community, carrying with it seeds of civil unrest. Some administrators will decide to forbid any use of social media but that may not be the wisest course of action to take. Police managers should not forestall subordinates' use of

---

[11] *Guardian Civic League, Inc., et al. v. Philadelphia Police Department, et al.* (2009, July 15) in United States District Court for the Eastern District of Pennsylvania. Page 19. Retrieved October 17, 2009 from http://www.whyy.org/news/itsourcity/complaint.pdf

[12] *Guardian Civic League, Inc., et al. v. Philadelphia Police Department, et al.* (2009, July 15)

[13] Post, David. (2009, July 26). The Volokh Conspiracy - More From the City That Brought You the First Amendment. Message by "Authur Kirkland" posted at 7.26.2009 2:15 pm to <http://volokh.com/posts/1248534075.shtml>

social networking technologies because to be effective enforcers of the peace in the Technology Age, officers must become as familiar with *online* communities as they are with brick and mortar communities. Instead, managers should develop policy that guides officers to maintain professional demeanor when using social media applications.

In Cops2.0, guest blogger Lauri Stevens describes seven core principles officers should be mindful of when using social media applications. Summarized, they are:

> **Integrity.** Whether on- or off-duty, officers should strive to be ethical and honest in their communications, remembering that they are held to a high standard in the community.
>
> **Use Disclaimers.** Officers should clearly identify comments as their own.
>
> **Identity.** Officers should use their real names when representing their agencies.
>
> **Department-sanctioned tools.** Officers should be encouraged to use agency-approved social media and their use should be closely supervised.
>
> **Competence**. Officers should demonstrate proficiency in their use of social media applications.
>
> **Command staff responsibility**. Police managers and administrators should avoid using publicly accessible social media to communicate with officers and staff.
>
> **Training**. Agencies should provide social media training for officers and staff. (Stevens, 2009)[14]

Social media applications have profoundly changed the way the world communicates. There is no going back. Law enforcement must adapt or risk becoming obsolete. Proper training and well-crafted use policies will make it possible for police to better serve their communities, both in the corporeal world and the online one.

[14] Stevens, Lauri. (2009, August 17) Guest post: Social media policies for law enforcement. Cops2.0. Retrieved October 24, 2009 from http://cops2point0.com/2009/08/17/guest-post-social-media-policies-for-law-enforcement/

Social Media:
Considerations for Background and Internal Affairs Investigators

Police managers intending to conduct inquiries involving employees' use of social media or to review applicants' social networking web sites should be aware of legal ramifications and potential exposure to civil suit, especially if it is decided to compel employees or applicants to provide user identification and passwords to their social networking sites.

> A search is constitutional if it does not violate a person's "reasonable" or "legitimate" expectation of privacy. (Katz v. United States, 1967)[15] This inquiry embraces two discrete questions: first, whether the individual's conduct reflects "an actual (subjective) expectation of privacy," and second, whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable.'" (US Department of Justice, 2002)[16]

There is as yet no hard and fast guideline that clarifies whether an expectation of privacy in electronically stored information is constitutionally reasonable:

> To determine whether an individual has a reasonable expectation of privacy in information stored in a computer, it helps to treat the computer like a closed container such as a briefcase or file cabinet. The Fourth Amendment generally prohibits law enforcement from accessing and viewing information stored in a computer without a warrant if it would be prohibited from opening a closed container and examining its contents in the same situation. (U.S. Department of Justice, 2002)[17]

Traditional Fourth Amendment principles, such as those governing closed containers, apply to digital evidence. Background investigators, in their eagerness to examine applicants' social networking sites, should not lose sight of the fact that even during a home visit, investigators cannot read personal diaries and correspondence, flip through photograph albums, or peruse documents stored in file cabinets. Neither should they capriciously inspect digital files stored on an applicant's computer.

---

[15] *Katz v. United States,* 389 U.S. 347, 362 (1967). Cornell University Law School, Legal Information Institute. Retrieved October 7, 2009 from <http://www.law.cornell.edu/supct-cgi/get-us-cite?389+347>
[16] US Department of Justice (2002) *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.* United States Department of Justice, Computer Crime and Intellectual Property Section, Criminal Division. Retrieved October 7, 2009 from <http://www.cybercrime.gov/s&smanual2002.htm#_IB_>
[17] U.S. Department of Justice, (2002)

Several federal statutes govern access to and disclosure of certain types of digital information:

- Electronic Communications Privacy Act
- Wiretap Act
- Pen Register and Trap and Trace Statute
- Stored Wire and Electronic Communications Act
- Privacy Protection Act

State statutes may be more restrictive than corresponding federal laws. Police managers should be familiar with both federal and state statutes because violations may result in evidentiary challenges or civil suit.

Some data stored in social networking sites may be privileged or protected. For example, the site may contain references to religious texts, discussions about religious beliefs, or messages from a religious advisor. The user in question may have exchanged email with an attorney about a lawsuit or the drafting of a will. The user may have received a text message sent via a smart phone from his physician. Investigators should take care to be cognizant of the potential for privileged information to exist on social media sites under review and to comply with applicable legal limitations regarding such information. One way to reduce risk would be to have an independent reviewer examine social media of applicants and report findings that do not include privileged or protected class information to the hiring board.

In the course of conducting a review of an individual's social networking sites, evidence of a crime may be discovered. In that case, the investigator should immediately discontinue the review, treat the computer as a digital crime scene, and obtain a search warrant. For a basic overview of issues regarding care and handling of digital evidence, see *Electronic Crime Scene Investigation: A Guide for First Responders* (http://www.ojp.usdoj.gov/nij/pubs-sum/187736.htm). The potential to follow up on any criminal cases that may be discovered are not likely to be compromised if reviews of social media sites are treated as if they were criminal investigations from the onset.

Employees or applicants who feel they have been discriminated against or wrongly accused of misconduct may opt to file complaints under the National Labor Relations Act, Civil Rights Act, or claim whistleblower protection. Clear and concise policies that both guide and protect investigators are needed to help guard against federal and state privacy law violations. Carefully drafted, well thought out consent forms are also needed to ensure applicants, employees, the agency and its investigators are protected.

Investigative Policy and Procedure

Procedure and policy for gaining access to applicants' and employees' social media websites are not yet standardized. Prudent administrators will proceed with caution, remembering that an agency's need to know does not outweigh applicants' or employees' rights to privacy. Investigators should not cast aside training and standard investigative practices for lack of commonly accepted policies and procedures for social media investigations. There is no excuse for investigators to act outside of their existing training. Human resource background investigators are currently exploring three approaches:

- To request user IDs and passwords so that they can log into "private" compartments of social media websites
- To eschew pass code access and to only search for and examine publicly accessible social media sites.
- To have the applicant or employee add the investigator as a "friend" to gain access to private sections of social networking sites.

The agency should work with legal counsel to ensure that consent forms are carefully drafted, taking into consideration nondisclosure outside the agency or human resource provider, and include limitations (such as not following links to other sites including "friends" sites).

Procedural guidelines should also alert investigators to be aware of and adhere to third party providers' terms of service (TOS) agreements. For example, both "Facebook.com" and

“Google.com” TOS agreements restrict users from certain activities. Facebook's "Registration and Account Security" TOS stipulates:

> 1. You will not ... create an account for anyone other than yourself without permission.
>
> [...]
>
> 6. You will not share your password, let anyone else access your account, or do anything else that might jeopardize the security of your account. (See <http://www.facebook.com/terms.php>)

Google's "Passwords and Account Security" TOS state:

> 6.1 You agree and understand that you are responsible for maintaining the confidentiality of passwords associated with any account you use to access the Services.
>
> (See <http://www.google.com/accounts/TOS>)

Investigators should also refrain from expanding the review outside of the user’s website, for example, by clicking on links, activating video or audio files, or visiting the user’s friends’ social media sites. Finally, investigators should be aware that a user’s site may have been altered by an unauthorized intruder who cannot easily be identified. By adhering to carefully drafted operational policy, agencies can avoid hiring discrimination claims and still conduct thorough background or internal investigations of social media sites.

The Execution of Four Police Officers:

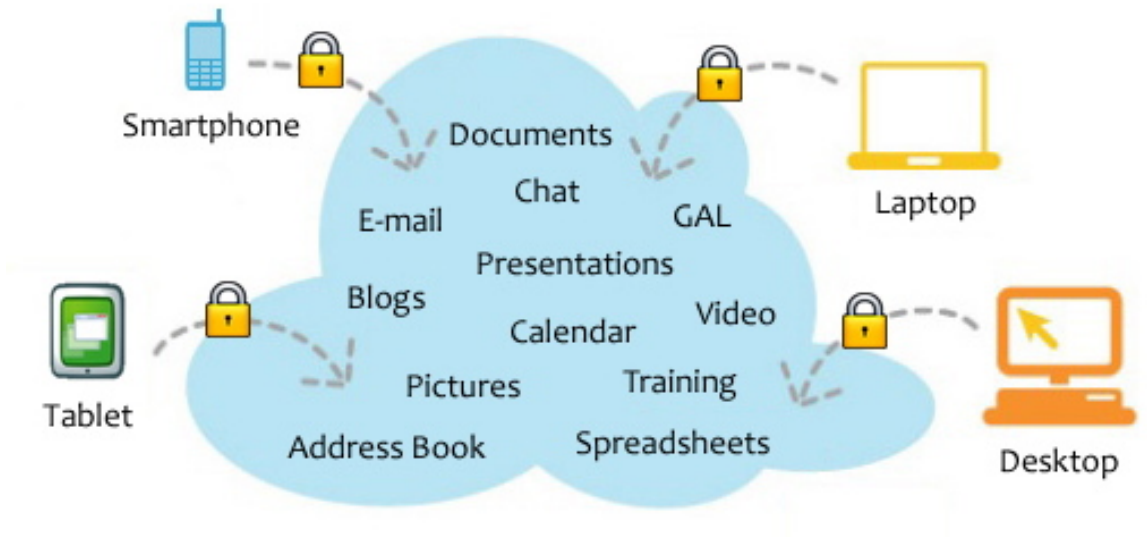
Lessons from a Social Media Tempest

Toby M. Finnie and Earl Moulton

The Nov. 29, 2009, murders of Sgt. Mark Renninger and Officers Tina Griswold, Greg Richards and Ronald Owens were the worst incident of violence against law enforcement in state history, and the manhunt that followed was the largest fugitive search in state history. — Seattle Times

Whether local, national or international, high profile events capture the public's attention and arouse desires to participate in meaningful ways. Social media enables and facilitates community participation at levels heretofore unimaginable. Websites such as Twitter, Facebook, Flicker, and Youtube were primarily designed for online socializing. However, these and other applications and web sites also empower users caught up in crises to share text, image, video, and audio files in real time. This sharing occurs well before public information officers or conventional news media can obtain, process and publish the data. These Web 2.0 tools have turned passive observers into active reporters. No longer content to stand submissively behind the crime scene tape, today's net-savvy citizen journalists can unflinchingly insert themselves into investigative processes, sometimes enhancing and sometimes interfering with police operations.

In Washington state, the execution-style murder of four police officers and the ensuing search for the fugitive shooter ignited a firestorm of social networking activities and introduced a new paradigm for law enforcement: It's no longer crowd management; now it's *cloud* management.



The Internet "Cloud"

Case Study: The Incident

At 8:15 AM on a quiet Sunday morning, Maurice Clemmons strode in to a coffee shop, shot and killed four uniformed Lakewood police officers while they worked on their laptop computers. It was a targeted attack against the patrol squad and their sergeant: Sgt. Mark Renniger and Officer Tina Griswold were killed before they could react. Officer Ronald Owens was killed as he physically engaged with Clemmons. Police determined that Officer Greg Richards also struggled with Clemmons and fired his weapon, wounding Clemmons (it was later confirmed), before being shot and killed. Witnesses observed Clemmons getting into the passenger side of a white pickup truck and fleeing the scene. A 40-hour long multi-jurisdictional manhunt ensued involving 600 officers from 16 local, state, and federal agencies.

The *Seattle Times* newspaper gave wide coverage to the crime and its aftermath, both in print and online, using social media tools such as Twitter, Facebook and "Google Wave," an experimental web application (with further development currently suspended):

> A Google Wave started by the *Seattle Times* is being used to track information about the search for a man suspected of killing four police officers. It's the first Google-supported manhunt and finally a decent use for Wave.
>
> Due to Google Wave's real time updating capabilities, this is actually a rather fitting use. People are posting everything they know, from information about the suspect (right down to his old pictures and Twitter accounts) to news from police scanners. A Google Map of the manhunt is also being maintained with the major events of the search. (Golijan, 2009)

Gripped by the unfolding drama, citizen journalists immediately began posting brief messages to Twitter accounts, including the hashtag "#WAshooting" set up by the *Seattle Times*. Editors credited ten staffers' tweets with driving a record-breaking 3.3 million page views to *Seattletimes.com*, using the linked Twitter account to push updated information out to readers (Cook, 2009). The success of the *Seattle Times* in driving traffic, and thereby revenue, means that this model is a permanent, not ephemeral, phenomenon. The result was a powerful information flow, combining resources from several media outlets, government entities, and ordinary citizens who added first person insights.

The first indication of a paradigm shift in crisis management arose early in the hunt for the fugitive. An hour after the shooting, a pickup truck matching the description of the vehicle used in the getaway was spotted in a parking lot near the crime scene:

> Streets around the coffee shop were blocked off late Sunday morning, and a police helicopter hovered over a large crowd of investigators. TV video showed police taking possession of a pickup truck parked in a grocery store in Parkland (Johnson, 2009).

Passersby noted the intense interest by the police and used cellular phones to snap pictures of the pickup truck and upload the images to Facebook, Twitter, Flicker, personal blogs, and other social media accounts. Before law enforcement could send out a press release and before the media could edit and broadcast the videotape, images of the truck were 'out in the wild.' This clearly raised the likelihood that relatives and friends rendering aid to the fugitive might learn about and alert him to the discovery of the abandoned pickup truck. On the other hand, the

information served to notify the citizenry to discontinue the crowd-sourced search for the vehicle and to slow the unrelated reporting of white pickup trucks flowing to law enforcement.

An additional piece of information about a 'person of interest' broke on the Internet before law enforcement had an opportunity to publicly announce it. In an after-event analysis, Renay San Miguel (2009) explained:

> The *Seattle Times'* fact-checking and source-working came to the fore Sunday afternoon, when its Web site ended up identifying a suspect -- before the Pierce County Sheriff's were ready to reveal that information. …In between updates from Pierce County Sheriff's spokesperson Ed Troyer, I checked SeattleTimes.com and saw on the front page that reporters had confirmation on a suspect name -- Maurice Clemmons, a 37-year-old with a long string of convictions in Arkansas and Washington states. However, Troyer had yet to name a suspect. I'll swear on a stack of Associated Press stylebooks that mere seconds after that story appeared online, reporters at the command post were getting text messages from assignment desks, and tweets were flying with links to the story.
>
> Troyer was forced to step to the microphones about 15 minutes after I noticed the Web page, confirming the Times' story by saying something to the effect that "we had to do this before we were quite ready."

At a televised press conference, Pierce County Sheriff Public Information Officer Ed Troyer announced:

> "I know that some of you have had this name, and I appreciate that you held back on it until we did some operations because we don't want to get anybody hurt or jeopardize it. We're still in the middle of those operations but we know the cat is out of the bag (so to speak) on his name, so we wanted everybody to have it at once. ...We're not going to elaborate anymore; you guys know we can't. We weren't even totally ready to do this yet. We wanted a bit more time to confirm some things; we're still in the process of confirming things. We want to make sure that we have everything accurate and, at this point, that's what we're saying, that he's a person of interest. I can't change it until we get more information and that may happen very, very quickly." (TyneRoseMedia, 2009)

The availability of sensitive information on the Internet poses ongoing issues for law enforcement. The very legitimate concerns alluded to by Troyer remained even after confirming the suspect identity. With the benefit of hindsight, it is useful to ask what law

enforcement purpose or duty was served by confirming the identity of the suspect prior to meeting law enforcement needs.

Asking "Whose purpose was served?" creates another perspective. The question suggests that the reporters 'forced' Troyer's announcement to meet their needs. Just as the *Seattle Times* website had already done, those reporters were free to report the identity without confirmation, but were seeking confirmation to meet their needs for liability purposes. In making the difficult choices like these in mid-crisis, it may be useful to reflect on the different audiences being reached by different forms of information release. In this case the release to mainstream reporters likely would reach a much larger local audience than that reached by the various Internet sources.

That the Internet sources proved accurate needs to be acknowledged. As an earlier study has demonstrated, *ad hoc* groups of individuals aided by social media tools are entirely capable of assessing complex data sources and arriving at accurate conclusions (Vieweg, et al, 2008). The self-correcting nature of social media use is illustrated by a BOLA tweeted by the *Seattle Times*:

> "RT @dlboardman: Cops looking for green 1997 Mazda Millenia WA license 208SSX registered to Clemmons' wife."
>
> — #washooting / carnitos/Mon 30Nov2009 20:14:20 +0000

That posting was retweeted numerous times, then canceled with an updated tweet from KIRO TV:

> "Police no longer looking for _1997 Mazda Millenia - WSP Trooper Brandy Kessler says it was sold 2 months ago"
>
> — #washooting / KIRO7Seattle /Mon 30Nov2009 22:54:02 +0000

In the meantime, media staff and citizen-users continued to provide images, links and commentary at a fast and furious pace. For example, about 500 Google Wave participants had access to the following information:

- Links to relevant Twitter accounts
- Description of the suspect that included a mug shot, possible aliases and a link to the suspect's (presumed) Twitter account
- Names of schools placed on security lockdown
- A copy of a bulletin issued by a university advising that campus police were following up on a tip and searching the grounds. Students and faculty were advised to be alert and especially aware of their surroundings
- Links to police scanner traffic sites on the Internet
- Links to video feeds on news media and Youtube.com sites
- Information about victims' memorials, including links to Facebook and Myspace
- Links to donation sites for victims' families
- Identification of areas under law enforcement surveillance or searches
- A real time chat area for users to share information

The barrage of online posts and uploaded files had potential to jeopardize police operations, threaten officers' safety and compromise investigations. "News organizations sometimes took their staffing cues from what residents sent in from smartphones or computers. …A citizen tweeted about cops searching on their street; KING [TV] sent a nearby reporter to check it out" (San Miguel, 2009).

> Tweeted on #washooting: "I can't believe they're by my house! UWPD has now arrived at Cowen Park and they closed down part of the street!"
>
> — AtomicPunk, Mon 30 Nov 2009 12:59:45 +0000

Seattle playwright Paul Mullin read through 5710 Twitter entries (#WAShooting, n.d.) in a post-event analysis of the social constructs that had formed. In an interview with KUWO

producer Jeremy Richards, Mullin commented that certain posts began to stand out from others. He noted that whether information was accurate or not, some people began to act upon it:

> Somebody showed up at Cowen Park after seeing on Twitter that police thought Maurice Clemmons might be there — and this guy showed up at Cowen Park in body armor, with a pistol! Needless to say, the police were not happy about this. (Richards, 2011)

Another web site, *Seattlecrime.com,* following and reporting on Seattle police's scanner traffic, produced a more detailed version of the Cowen Park incident:

> UPDATE @ 12:30 p.m.: Police are forming a perimeter around Cowen Park and pushing gathered members of the media back from their positions. Apparently traces of blood were found in a bathroom in the park. Scanner chatter indicates police are closing off segments of Brooklyn Ave. in the U-Dist.- Ravenna area to pedestrians and car traffic.
>
> UPDATE 1:44 PM: A man who was wearing body armor and packing a pistol showed up at Cowen Park. Police briefly detained the man, who has a concealed weapons permit, as it is apparently illegal for those not in law enforcement to possess such armor. We agree with the P-I's Casey McNerthney when he tweeted: "Reports of man with body armor shows up at Cowen Park to help. He didn't help." (Spangenthal-Lee, 2009)

Law enforcement has long understood the impact of radio scanning and made encryption and radio protocol decisions accordingly. However, those decisions may need to be revisited. In the social media world, a single individual listening to a scanner has an effect amplified by posting radio transmissions on social media.

Twitter post to #washooting: "They're complaining about the Times' photos on scanner."

— AtomicPunk, Mon 30 Nov 2009 12:59:45 +0000

Police were also displeased with a photographer who worked for the *Seattle Times.* According to Mullin:

> Cliff DesPeaux, a photographer who was an intern with the *Seattle Times,* was at one of the locations that the Seattle SWAT team had surrounded, thinking Clemmons was inside. It was utterly dark, so dark that the other photographer DesPeaux was with

> couldn't get any pictures. But Cliff had a new camera that he was shooting shots with — that he was just pointing at the dark — and when he looked at his viewfinder, he could see that the SWAT team was moving in on this house at three in the morning.
>
> He's tweeting from the scene; his Twitter followers explode from seven to 700; CBS news is tweeting him, asking him to call them at their headquarters in New York City. And then he gets a call from the *Seattle Times* saying, "You need to stop tweeting or at least you need to stop tweeting police activity in an ongoing manhunt."

> Twitter post to #washooting: "Ed Troyer Pierce County Detective just spoke to @Q13Fox at 9 channel 110 on comcast. Asked people 2 not report their movements"
>
> — virginiagriffey, Tue 01 Dec 2009 02:38:18 +0000

Mullin further explained:

> Basically what had happened is that the Seattle Police were following DesPeaux's Twitter feeds (because the *Seattle Times* was running it live at their web site). What they [the police] said to the *Times* which the *Times* then passed onto DesPeaux — who was a young guy who didn't know any better — *You don't cover what the police are about to do.* You can cover what they're doing and you can cover what they've done but if you're tipping their hand as they're trying to move on in on a dangerous armed criminal…. You know? That's *bad!*

The element of surprise necessary in some police operations is losing out to social media. Police must assume that criminals will monitor social networking sites to learn — as best they can and in real time — what police are up to.

Two further lessons present themselves from DesPeaux's actions. The first of these may provide some cold comfort to law enforcement managers. The management of the *Seattle Times* is facing, and having as much trouble dealing with, the changes created by social media. Their training and acculturation processes are clearly inadequate to meet their own needs. The second lesson comes from the technology itself. The technology that revealed the SWAT movements is also available to criminals. That changes how SWAT needs to conduct operations. It may become necessary to re-think the distances required for operational perimeters in order to protect against such use. The advancement of technology means that all aspects of law

enforcement response need constant re-assessment. The length of time that a Standard Operating Procedure remains relevant is rapidly approaching zero.

Not only were police communications being monitored, but also fire and rescue broadcasts. Some individuals attempted to learn access codes to more sensitive police communications — and other users responded with suggestions:

Twitter posts to #washooting:

"SPD SWAT operations channel still ellusive to me. Anybody know the radio frequency / talkgroup they are using" — esl_zone, Tue 01 Dec 2009 07:41:42

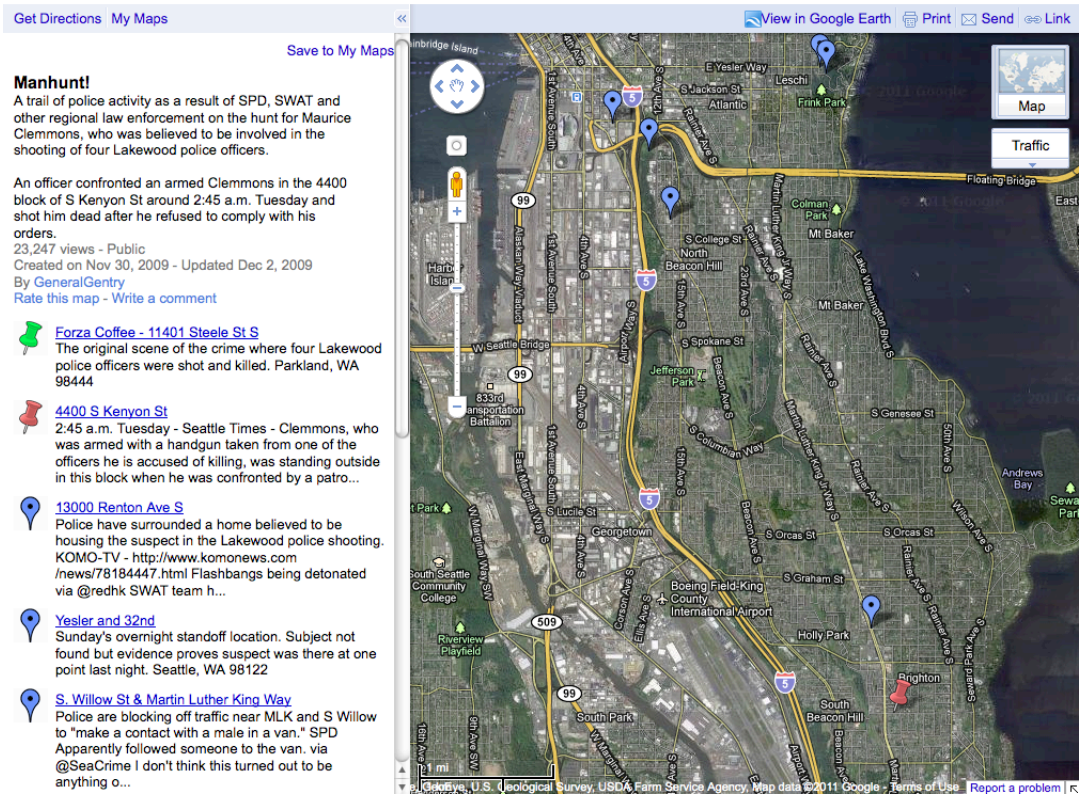
"@esl_zone here is a link with all the different freq's for SPD http://www.radioreference.com/apps/db/?sid=604" — akfirefighter, Tue 01 Dec 2009 07:47:00

@esl_zone here's link to trunk freqs http://www.muppetlabs.com/~chris/scanner/trunk.txt — 200TMaster, Tue 01 Dec 2009 08:48:29

These tweets show an additional complexity of the social media reality. Not only are law enforcement objectives jeopardized by members of the public, partners in emergency response can create information leaks. Both the intentional tweets made by fire and ambulance services for their own purposes and the leaks by their onsite personnel, all of whom are carrying social media-enabled devices, are beyond the control of law enforcement policies and protocols. Understanding those risks for each other is one of the new duties of all emergency response personnel.

Created with web-based applications such as *Dipity.com* timelines followed events from one city to another, story by story, video by video. Digital "pin" maps displayed up-to-the-

minute activities and geographic locations of police operations.



Police Response Tracking Map using Google Wave Application (GeneralGentry, 2009)

Multiple posts from the Twitter account "#washooting" describe events involving the fugitive Maurice Clemmons and his final and fatal confrontation with Seattle Police Officer Benjamin Kelly on Tuesday, December 1, 2009 at approximately 2:45 AM.

Archived posts to #washooting (2009) (Note: user names and timestamps have been omitted but messages otherwise appear as posted):

Possible suspect male black with mole on face 4430 South Canyon St possible capture happening nowless than 5 seconds ago

All units are responding to that location. Sounds like they think they have him.

Guild rep has been requested... Suspect probly shot

They got a suspect matching his description on the ground right now. Possible they might have him!

They are callin in MEDIC to the scene of this suspect!!! Please tell me they just got him!

Scanner listeners... be sure to turn on SFD AMR and hospital freqs for suspect condition. He has been shot by SPD

The shooter from Lakewood has been shot at 42nd

Suspect in route to harborview...

Scanner people: Monitor Harborview and SFD freq. SPD riding with suspect to Harborview

Command post is goign to be setup on scene this looks like it is it!

45th and Kenyon. SWAT moving in. Scanner mentioned suspect going to Harborview. Is this it?

Scanner is getting quiet... channell 3312 is opened! containment is done! it is over!

They are joking and laughing on scanner police seem happy! Suspect vehicles been looking for 2x at residence.

Law enforcement source confirms suspect arrested on 4400 block of S. Kenyon was Maurice Clemmons.

Possible officer involved shooting in the 4400 block of S Kenyon. PIOs Kappel and Whitcomb enroute to the scene.

Epilogue: On December 1, 2009, Twitter user Erik M. Hicks ("@emhicks00") posted the following message:

IMAGE SOURCE: http://twitter.com/#!/emhicks00/status/6254726791

Responding to an inquiry from David Quinlan, KIRO TV, "emhicks00" wrote:

IMAGE SOURCE: http://twitter.com/David_Quinlan/status/6285059601

As with so many "facts" on the Internet, the source of the photo uploaded by "@emhicks00" is not necessarily a postal inspector:

> Forgive me, but that's about as close to segueing back into Christmas Season as I'm likely to get this week. Right now, I can't offer anything much more cheerful than a picture of a dead cop-killer, forwarded by a brother in the northwest. (Cops have cell phone cameras too) (Ayoob, 2009).

Internal affairs investigations were launched in police, fire, and medical examiner's offices in an attempt to determine the individual responsible for obtaining and publishing online a picture of the deceased suspect, Maurice Clemmons.

Implications for Law Enforcement

Whether it's pursuit of a wanted suspect, rescue of a lost child, or response to a natural disaster, social media networking enables ordinary citizens to become invested in the narrative whether crisis management supervisors want them to or not. In his emergencymgmt.com blog, Gerald Baron contends that "It's not your response anymore — it's theirs." (Baron, 2011 April 12) Perhaps a more practical and useful concept is that the advent of social media emphasizes what has always been true: At base, the response of emergency services needs to be understood as 'ours.' All the players have needs and aspirations and all of those need to be under active consideration in any emergency response.

Internet savvy users are no longer content to wait for "news at eleven." Incident commanders and public information officers must find ways to use social networking tools to accurately inform the public, dispel rumors, monitor for actionable intelligence and generate trust. Whichever ways that an agency may discover to use social media, they will need to understand the reason that social media is powerful and so effective. The history of communications up to the advent of the Internet was about the progress of moving from one-to-one communication to one-to-many technology. Social media has added the capability for

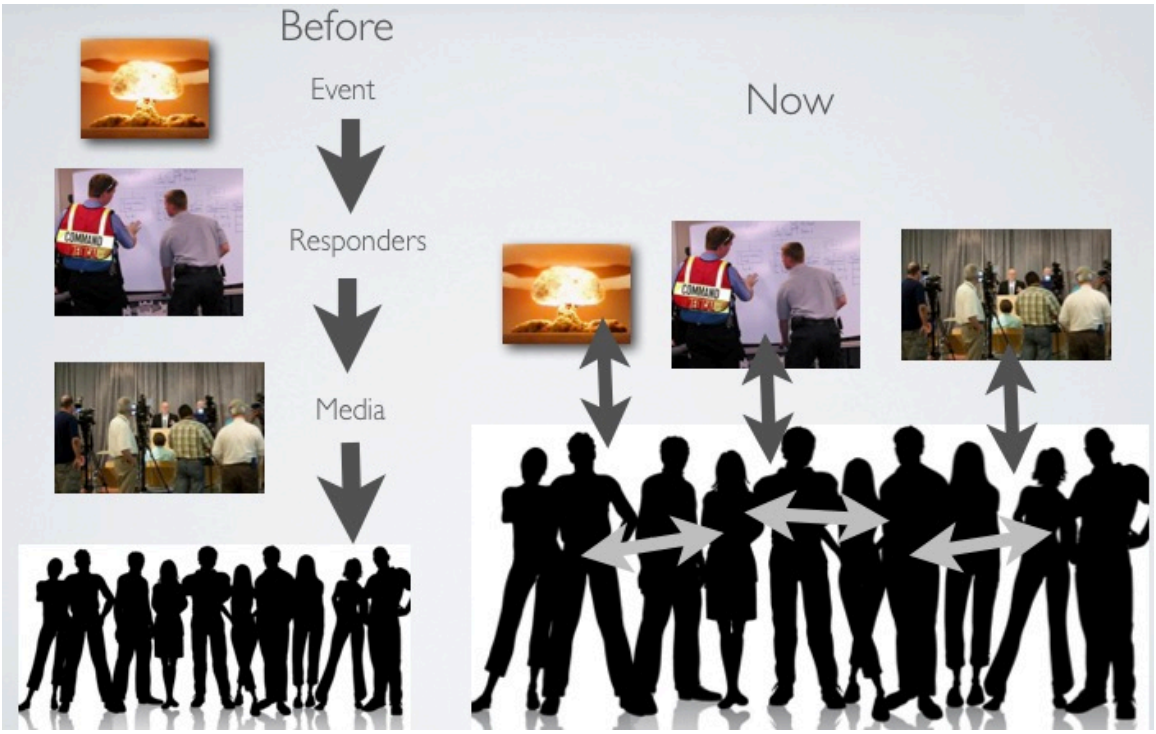
one-to-all communications while retaining the capabilities for one-to-one and one-to-many communications. This evolution has been coupled with the complete lack of any capacity issues to create the social media world.

The social media world is not confined to a particular group of participants. The social media world is not confined to particular kinds of information. The social media world is not confined to any particular geography, jurisdiction, nation state, language or time zone. Because so much of the citizenry have harnessed the power of the social media world in their private lives, they have formed the entirely reasonable expectation that their public institutions will do the same.

Crisis and emergency communication planning today must include a process for managing interaction. Chief Bill Boyd, City of Bellingham Fire Department describes the challenges:

> The days of a Public Information Officer (PIO) sitting down at a computer and generating a two paragraph media release a couple of times a day, and an interview here and there are gone. If you still think this is all the PIO really has to do then you might as well give them an old typewriter and carbon paper. As an Incident Commander (IC), I "define the box" the PIO will operate within (giving them the flexibility and boundaries to immediately release information without me having to approve it). The IC needs to immediately set policy, validate key real time message concepts and then do the most important thing- let the PIO loose to do their job. As an IC in this day and age, I can ill afford to get further behind the information dissemination curve (assuming we are already behind thanks to social media, camera cell phones, etc.).
>
> This also means PIOs must be skilled in creating short messages, and relaying them in the most succinct way (how would you relay an evacuation order on Twitter?). In the major events I have been involved with over the years, this type of messaging was not available. Now, it is the preferred method of communication by many. Yet, it remains foreign to many in the emergency response community.
>
> ICs need to wake up and realize the impact of the explosive growth of social media and the resulting expectation for immediate and accurate information. If the public does not get it from Incident Command they will get it from somewhere else, relay inaccurate information and/or undermine your authority by venting their frustrations about lack of information (Baron, 2010).

Social media networking has forever changed incident commanders' and public information officer' roles. Forward-thinking leaders will find ways to integrate social media networking into crisis communication operations. In constructing these new approaches, those leaders will need to consider two primary aspects of the social media world. A primary attribute of social media is that it occurs in real time. As the graphic below illustrates, there is virtually no time lag between events in the real world and the reporting of those events in the virtual world. Any integration of social media into law enforcement's responses during crisis must give full effect to this reality.



Source:

http://media.govtech.net/BlogFeeder/CRISIS_COMM/Before_Now_Public_Info_Graphic.png

A second primary aspect of social media is that communications in social media forums become moderated by particular users that are trusted by the wider user community (Vieweg, 2008). This aspect holds a number of implications for crisis managers. First, in order to be trusted, a user needs to be known for providing good information. What this means is that it is possible for agencies to establish their presence in various social media communities in advance. By properly maintaining that presence, an agency can mediate what information gets shared and where that sharing takes place. Having established trust in advance, an agency can leverage that trust during a subsequent crisis event.

Traditionally, policy makers have looked at a problem, researched it, developed a policy and then moved on to the next issue. This model will not work when dealing with social media. The Internet is constantly creating new, and re-creating older, functions. Even the people who design these functions do not and cannot fully anticipate all the uses to which a function will be put. For example, the use of Twitter as a command and control mechanism for activists was as unanticipated by its creators as by law enforcement. The implication of the constant change and expansion in the social media world is that understanding, leveraging and responding to those changes requires a similar flexibility in policy. The very concept of flexible policy will be viewed by some as an oxymoron but is nonetheless an absolute requirement.

A similar flexibility may be required in respect of agency personnel who may be expected to have to deal with social media. The practice has evolved in emergency response agencies to appoint particular individuals or units as media relations or public information officers. That practice evolved to meet the needs and requirements of mainstream media. However, mainstream media has remained relevant only to the extent that it has embraced the tools and techniques of social media. Consequently their needs can now be met by an agency's competent use of social media. This observation also leads to the conclusion that individuals who may have been selected for PIO duties based on their ability to meet mainstream media needs may not be the right individuals for effective communications in social media. It may even be time to consider whether communication via social media is the job for someone or is it some part of everyone's job.

The speed and volume of information that emerges in crisis situations on today's Internet carries with it significant problems for law enforcement. Our ability to mitigate the challenges and to leverage the opportunities will be reflected by the degree that an agency embraces the positive aspects of the Internet. People, policies and procedures in policing need to be flexible. They need to be continuously connected to multiple sources of information. And they need to be able to respond in Internet time: immediately.

References

#WAShooting Tweets - the hashtag that tracked Maurice Clemmons. n.d. *The New News: A Living Newspaper.* Retrieved from: http://www.newswrightsunited.org/productions/WAShooting_Tweet_Archive.xls

Ayoob, M. (2009, December 7). In a season of love, undercurrents of hate. *Backwoodshome.com,* Retrieved from: http://backwoodshome.com/blogs/MassadAyoob/2009/12/07/in-a-season-of-love-undercurrents-of-hate/

Baron, G. (2010, March 1). An incident commander asks: Does ICS mean information communications standstill? *Emergencymanagement.com.* Retrieved from: http://www.emergencymgmt.com/emergency-blogs/crisis-comm/An-Incident-Commander-asks.html

Baron, G. (2011, April 12). It's not your response anymore — it's theirs. *Emergencymanagement.com.* Retrieved from: http://www.emergencymgmt.com/emergency-blogs/crisis-comm/Its-not-your-response-041311.html

Baum, D. (2006, January 9). Deluged. *The New Yorker* Retrieved from: http://www.danbaum.com/Nine_Lives/Articles_files/%22Deluged%22.pdf

GeneralGentry. (2009, November 30). Manhunt! *Maps.google.com* Retrieved from: http://maps.google.com/maps/ms?hl=en&ie=UTF8&msa=0&msid=100100228202640074527.0004799a6df0cb005bdf5&ll=47.624099,-122.284184&spn=0.083303,0.154324&z=13

Golijan, R. (2009, November 30). First made-for-Google manhunt in progress. *Gizmodo.com.* Retrieved from: http://gizmodo.com/#!5415608/first-made+for+google-manhunt-in-progress Cook, John (2009 November) *Techflash.com.* Retrieved from: http://www.techflash.com/seattle/2009/11/washington_police_shootings_a_watershed_moment_for_twitter.html

Johnson, G. (2009, November 29). Police looking for person in shootings. *The Seattle Times.* Retrieved from: http://seattletimes.nwsource.com/html/localnews/2010385761_apusofficersshot20thldwritethru.html

Martin, J. (2010, April 24). A path to murder: The story of Maurice Clemmons. *Seattle Times Newspaper*. Retrieved from: http://seattletimes.nwsource.com/html/localnews/2011695929_clemmons25m.html

McHale Testimony. (2005). Paul McHale, Assistant Secretary of Defense for Homeland Defense, testimony before a hearing on Hurricane Katrina: Preparedness and Response by the Department of Defense, the Coast Guard, and the National Guard of Louisiana, Mississippi, and Alabama, on October 27, 2005, House Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, 109th Congress, 1st session, 74.

Richards, J. (Producer). (2011, February 12). Tweeting the manhunt: an interview with Paul Mullin. *KUOW Presents.* Podcast retrieved from http://www.kuow.org/mp3high/mp3/KUOWPresents/20110212PaulMullin.mp3

San Miguel, R. (2009, December 4). A painful social media foray for Seattle journalists. *TechNewsWorld*. Retrieved from: http://www.technewsworld.com/story/68805.html?wlc=1306604236

Spangenthal-Lee, J. (2009, November 30) Maurice Clemmons killed by police. *Seattlecrime.com*. Retrieved from: http://www.seattlecrime.com/2009/11/30/manhunt-continues-for-clemmons

TyneRoseMedia. (2009 November 29). Person of Interest in Police Killing's in Washington Has Extensive Criminal History (King 5 News Source). *Youtube.com.* Retrieved and transcribed from: http://www.youtube.com/watch?v=RAfRByPXGjo&feature=player_embedded#at=156

Vieweg, S., Palen, L., Liu, S.B., Hughes, A.L. & Sutton, J. (2008) Collective Intelligence in Disaster: Examination of the Phenomenon in the Aftermath of the 2007 Virginia Tech Shooting. Proceedings of the Conference on Information Systems for Crisis Response & Management (ISCRAM).

The Right to Accuracy: A New Frontier

Michael E. Buerger

Whether 'privacy' as we once understood it still exists remains a hotly contested proposition. Most of us have encountered the terse dismissal that "You already have no privacy; get over it." While we might cling to the desire for privacy, we daily encounter evidence that technology's Cambrian explosion has seriously eroded and redefined, if not eradicated, our old expectations of having control over information about ourselves.

The immediate impact on most Americans would seem to be targeted advertising, but there are more serious consequences of the widespread availability of personal data: identity theft is the one most commonly thought of, but in the interconnectedness of cyberspace, other negative consequences may result. Identity theft – the journalistic meme for a process better described as "identity appropriation" or "identity cloning" – can take several forms. Unauthorized digital 'identities' can be used to make credit applications, and then compile huge unpaid bills from purchases. Illegal immigrants use appropriated identity data as cover while working for U.S. companies. And some individuals adopt the cloned identity of others to escape an undesirable or unsavory past: some seek to shed criminal identities, others to escape abusive relationships, and perhaps some merely to start over.

Identity theft for financial gain creates considerable havoc for its victims, particularly when their cloned *personae* have run up enough unpaid bills to affect the real person's credit rating. Victims of this kind of identity theft recount tales of laborious efforts to clear their names, a process requiring many months if not years of painstaking reconstruction of their finances. For those citizens who discover that their identity was appropriated for other criminal purposes, immediate consequences (arrest, detention in jail, etc.) can be more severe, but the resolution is often faster and somewhat easier. Many identify theft victims describe circumstances very similar to the fictional scene at the resort hotel in the 1995 movie *The Net*,

in which the flesh-and-blood Angela Bennett tries to assert her identity to the hotel clerk, who repeatedly denies her because "the computer says" she checked out several days earlier.

How Quickly We Arrived Here

Older Americans inherited expectations of privacy that were forged in physicality. Closed doors, sealed mail, face-to-face conversations and confidences were the norm, and social conventions reinforced the expectations. All were protected at one time by the Fourth Amendment to the United States Constitution: the right of the people to be secure in their persons, property, papers, and effects… all physical entities. Private communications were protected by the Postal Service and by laws that criminalized tampering.

Private paper records once existed in one place. They were vulnerable to compromise, of course, through burglary, theft by employees, or erroneously being discarded. They were also vulnerable to destruction by flood, fire, or other means. At the core, the physical record – in a doctor's office, or at a local store – was maintained by one or both of the people involved. However, the advent of the photocopier (and more recently, cell-phone cameras) created a new hazard, loss of privately-held information without the loss of the original document to mark its passing.

In the last quarter-century, an alternative universe has overtaken the physical world. The telegraph, the radio, the telephone, and television were all harbingers: in fits and starts, they transcended the limitations of physical space. The computer age has knit them into a single entity – cyberspace – that combines all of their functions, creates new possibilities, and informs a young generation with social understandings far different from those of their forebears. Then paper files were transformed into databases and the older expectations of dyadic relationships disappeared as individual, cash-based transactions were replaced by a network of intermediaries: banks, credit card companies, insurance companies, and multiple layers of intermediary vendors. The system proliferated because of perceived benefits to the individual: time was compressed, usually to the benefit of the clients. The process needed to

duplicate and share large amounts of information changed from a laborious, time-consuming effort in front of a photocopying machine, to a simple series of keystrokes and clicks on a computer.

The unintended consequence of that transformation has been to make formerly private data semi-public. The process began long before the database, because the supposedly dyadic relationship between patient and doctor is not dyadic in fact. Insurance companies receive the information in order to determine eligibility for payment and all of the major actors may outsource portions of their operations to intermediaries. Bank records, credit card records, and other financial histories are compiled into credit histories and ratings that are available to individuals and corporations alike.

The Direction We Are Going

Seen in the most favorable light, such databases allow those who would extend credit (a commercial transaction) to make informed decisions on the likelihood of being repaid, reducing their risk of loss and theoretically improving the overall economy. As more and more information emerges about the quiet proliferation of data-sharing and data-mining intermediary corporations, the more the negatives emerge. Targeted advertising is the most visible manifestation, but subtle and overt efforts at social engineering ("People like you who bought this item also bought…") now provide an ominous undertone to communications from cyberspace.

With the advent of computerized records systems as the foundation of judgment, society inherits four sources of potential distortion of the records base:

1. human error upon entry;
2. computer-located error, resulting from coding errors, glitches in power sources, and degradation over time;

3. intentional distortion due to malicious hacking (often aimed not at the individual, but at the corporation hosting the database); and

4. unintentional distortion as a result of widespread virus and other malware distribution "in the wild."

Databases are inherently abstract: at the best of times, individual data entries are not accurate representations of the real individual whose name they bear, but rather selected slivers of information pertinent to the corporation or organization that originally collected the information. The *de facto* abolition of time in cyberspace compounds the problem. The Tralfamadorians in Kurt Vonnegut's *Slaughterhouse Five* might have seen humans as a long pink trail through time, but in cyberspace that temporal elongation is compressed into a single dense, bloated caricature of every second of the individual's life to date. Maturation, change of external circumstances, heroic efforts at self-improvement have no sway there, nor is there any discernible effort to identify or correct error (routine verification and corrective procedures may be in the primary databases, but once loose in the secondary market, it is unlikely that error could be identified: there is no financial incentive to do so and the presumption of accuracy reigns).

The Person whose name or number is contained in a database is represented there, but only by a series of numerical entries in preselected categories. Those categories are determined by private vendors for their own purposes and represent only the slender portion of the person's life that is of immediate concern to the corporate host. Whether those categories – and the values the entity ascribes to them for each individual – are precisely rendered or even common across the universe of databases in which they are compiled is far from certain. Even less certain is the degree of pattern and variability that they represent, in the singular for a particular vendor or in the aggregate when databases are merged.

Critical readers will no doubt object that a careful analyst would make allowances for the progression of time, but that is in fact one of the points of this essay: a "right to accuracy" requires such an effort be conducted, but human behavior is not that diligent. Sloppiness due to fatigue or distracted attention, slipshod work performed under conditions of ennui or

resentment (of boss, of station in life, of the way the world is going to Heck in a hand basket, etc.), all introduce unintended – and uncorrected – errors into databases. The rate of that error may be known to some, but is not widely disseminated; nor are particulars made available to those whose records are affected.

Two developments have arisen that cast even more baleful aspects on these records. This first is the corporate annexation of the data itself, claiming that information provided by an individual for the purposes of obtaining credit or to make a purchase under other arrangements becomes the solely-owned property of the corporation, divorced entirely from the individual that abstract set of data represents. The second is the use of the collected and linked databases – "Big Data," in the current parlance – for network analysis and intelligence gathering by enforcement agencies and agents.

Data-mining is the nexus of the private-public division. The poorly-named Operation Carnivore was premised on the federal government's ability to compile commercially-available databases and examine them for patterns that suggested (or verified) criminal activity. The specter of "Big Brother" rooting through the everyday transactions of private citizens was sufficiently repellant to force the termination of the program, despite the fact that corporate entities routinely engage in the same practice. In the movie *Minority Report*, speaking of the Pre-Cogs who predict murders before they happen, the character of Danny Witwer reminds us that "[t]he oracle isn't where the power is, anyway. The power has always been with the priests…even if they had to invent the oracle." Modern databases -- Big Data -- are the contemporary oracles, silicon equivalents of the Pre-Cogs in the movie: the belief that they can predict human activity is promoted by the priests of Big Data.

The most critical juncture is that of the decision: judgments are made about individuals based upon the compilation and 'smoothing' of multiple abstract representations, all without any contact with the actual person. Data are not 'facts,' necessarily, and all 'facts' are subject to interpretation in any event. That there may be no defense against a judgment made as a result of interpreting patterns in a database is troubling, raising the specter of a wrong decision, with

near-catastrophic consequences for the individual: in effect, constituting a 21st-century Court of Star Chamber.

The Right to Accuracy

If privacy is indeed an indefensible relic, applicable only to physical intrusion into a private residence or other structure, then invoking a 'right to privacy' is the wrong argument to pose against the perils of cyberspace. Those who defend Big Data correctly point out that most 'private' information is shared voluntarily, even eagerly, in order to obtain some goods or service in return: in that view, information has already been commoditized by the consumer. The counter-argument that it is all but impossible to live in the modern age without such transactions is accurate, but ultimately probably irrelevant. The generational shift to broad-scale exposure via social media is another aspect that erodes the notion of traditional Fourth Amendment protections for commercial data, though society is in the early stages of that transformation, and may yet arrive at different social practices if the harms threaten to outweigh the benefits.

What is needed in its place is a Constitutional right to accuracy, a concept that should include time-relevance as well as individual entry precision, among other concerns. There is a time-honored, well-used process for amending the United States Constitution to meet the emerging demands of a changing world; it is political, it takes time, and it does not always produce the desired results, but its practical and metaphysical clout is far more likely to produce positive incremental changes regardless of the ultimate outcome. While it is true that the Constitution protects citizens only against government action, such an amendment could well be fashioned to invoke, or coordinate with the Commerce Clause, and simultaneously empower government to extend comparable protections to citizens through regulation of the data markets. There are many, many issues and details to be worked out – not least of which is the burden of establishing the ability to verify the accuracy of billions of individual entries – but the process starts with the assertion. The next steps need to occur in the public domain, a series of conversations about the positives, the negatives, and the mechanics of creating a

system that protects us from having to defend our real selves against a simulacrum created by demons in the machine.

Bond-Relationship Disruption:

In Defense of Strategic and Tactical Deception

Sid Heal and Michael E. Buerger

To a lesser or greater extent, all human interactions rely on some form of trust. Criminal enterprises are no exception, though their interactions involve a different definition of trust than that which most law-abiding citizens would recognize. Street gangs, drug cartels, and other criminal groups have rigid codes of conduct, enforced by violence. This is a dark side of trust based upon predictability of behavior. While some might argue that these bonds are based on fear rather than trust, a closer examination reveals that fear is just the tool used to establish trust. It is not mutual trust, but a one-way relationship that allows criminal leadership to trust its subordinates. It is the confident assurance that failing to comply with the rules and expectations of those with authority will result in retribution. More importantly, the measures taken to enforce this trust are surer and far harsher than those of a government attempting to discourage it: it relies on sure and direct punishment, unencumbered by checks and balances, concerns about civil rights, or safeguards against error. The larger and more formal the criminal enterprise, the more persuasive this factor becomes.

A bond is thus formed between members and groups of a criminal enterprise that enables plans and transactions to succeed without the cumbersome written contracts that characterize business arrangements in the civil world. Crime lords can trust their confederates because of a combination of internalized loyalties and the very realistic fear of retribution for those failing to meet the minimum standards. We propose that even those bonds can be broken, or at least rendered less trustworthy, through a combination of technological improvement and social engineering. Admittedly, there are slippery ethical slopes inherent in the endeavor, but the law recognizes a balance under “competing harms.”

Bond relationship targeting is not just a new strategy, but an entirely different way of thinking. It has value, not just in serious criminal offenses, but in all types of criminal ventures. Traditional reverse sting operations have operated on the same principle as the options proposed below: if any on-street drug pusher, prostitute, or fence can be an undercover police agent, the thief's ability to rely upon 'trust' to complete a criminal transaction is seriously eroded. Reverse sting operations are time and labor intensive, however.

The remainder of this paper will highlight some of the concepts in the hopes of stimulating thought and ingenuity in deterring crime and making our communities safer with tactics that exploit new technologies as well as old. As with any tactics employed by agents of government, there are ethical and legal constraints to consider, but effective law enforcement often pushes the envelope of law, especially in new areas where technology creates new possibilities not envisioned in earlier eras. We offer these scenarios as think-pieces, not as panaceas.

Examples and Illustrations

Example #1: Radar Chirping

One simple illustration of the principle of bond relationship targeting involves speeding drivers intentionally avoiding the posted limits with the use of radar and laser detectors. In this case, the trust relationship is between a person and a piece of equipment. The likelihood of a motorist ignoring the posted speed limit is largely reliant upon their degree of confidence that the radar/laser detector will provide sufficient warning. The trust one places in such a device is a low-level 'bond' and without constitutional or human rights implications.

Attacking this bond relationship involves police departments employing portable and inexpensive transmitters, called 'chirpers,' that pulse radar and laser signals to intentionally set off the detectors purchased by the would-be speeders and in violation of the local speed limit. This method works in two ways. The first occurs with the slowing of drivers who are alerted of a potential law enforcement 'speed trap' when their detector signals them and they slow down

to avoid the penalties. The second occurs when drivers discover that police are using chirpers instead of actual radar or laser speed determination devices, because their detectors become less reliable for predicting when they are actually being targeted. In fact, the more often these detectors were falsely activated the less reliable they become, until at some point they could be considered completely worthless. Thus, the value of a technology built and used to defeat the legitimate efforts of government to gain compliance with a law could be completely negated without the necessity of legally prohibiting them and the accompanying cost and effort of enforcement.

Applying the principle to human interactions raises some other issues, but also suggests similar benefits. In this example, there are certain regulatory considerations (licensing the 'chirping' unit, for instance), but the potential benefits outweigh the initial expense and effort. Because the devices are 'send' only, with no calibration or court presentations involved, ongoing certification is negligible, and verification of frequency can be done in-house at limited expense.

Example #2: Property Identification

The bond between a thief and his "fence"[18] is an old one, paradoxically resting upon anonymity: the anonymous link between an item of stolen property and its rightful owner. The twentieth-century requirement that pawnshop owners and other dealers in second-hand goods keep records of the property attempted to mitigate this link, but was undermined by the anonymity of the thief. While the fence might very well know a thief's true identity, the use of false identification serves to fill the blank space in the ledger examined by the police and unless the police are physically present at the time of the transaction, the receiver of the stolen property would have a plausible, if thin, defense against charges of complicity. The illicit relationship is facilitated by the thief's trust that the fence will not reveal the identity of the person who pawned the item.

[18] As used here, a "fence" refers to a person who receives and disposes of stolen goods.

The expansion of technology has already limited this anonymity and more is in the offing. Property such as jewelry—difficult to mark with an owner-inscribed number (OIN) under earlier technologies—can now be labeled using laser technology, without destroying the esthetics of the item. Concealed RFID chips link specific items to specific owners. Although any electronic system is vulnerable to electronic countermeasures, it requires a greater investment on the part of the fence—the thief is unlikely to make such an investment—and the mere possession of equipment capable of altering RFID frequencies erodes the fence's claim to "honest mistake."

The advent of biometrics on a larger scale than is currently available will further strip the anonymity of the thief, especially if biometric systems make real-time reports to a property database monitored by algorithms or by the human eye. The lag time between theft and discovery may well be greater than that between the theft and fencing, so immediate apprehension may not occur. Notwithstanding, the benefit lies in increasing the certainty that the connection will be made at some point. At the very least, the fence loses the potential profit of property identified as stolen, as well as the funds already paid to the thief, not to mention the increased vulnerability for future ventures after even once been identified as a possible suspect.

The system will remain vulnerable to its greatest current weakness, the human laxness that fails to record serial numbers or identify valuable property with an OIN. Tightening the noose around property that is recorded nevertheless raises the potential cost to the thief, and to the fence. An ancillary benefit of the effort lies in the fact that what property is so protected, and what is not, is unknown to the fence. The greater gain will be that neither the thief nor the property will be as anonymous as before, and the bond of trust between fence and thief will be much more dubious.

Example #3: Collaborative Policing

One of the earliest forms of policing is called the "hue and cry" method. Dating back to at least the early middle ages, this method worked by summoning every able-bodied male within shouting distance to assist in the apprehension of a criminal. As the policing function became more capable the system has all but disappeared but residual forms still exist in the laws that allow private persons to make arrests, and posse comitatus.[19] Collaborative policing is a form of bond relationship targeting in which the bonds between members of the community and law enforcement officers are strengthened through collaboration. Similar to the popular community oriented policing model, collaborative policing is far more robust and describes an effort that actively involves citizens, especially victims, in the safety and well-being of their own communities. Consider the following example, which expands the stolen property example above.

Risk is the metric when measuring trust, with zero risk equating to complete trust and one-hundred percent equating to no trust. Hence, any manner of raising the risk degrades the trust bond necessary for a criminal enterprise.[20] In this case, a bond exists between the legitimate owner and his property because of his ability to identify and prove ownership. The bond is also increased in both ways when the owner finds and identifies his property and calls law enforcement for the appropriate enforcement action. At a minimum, the property owner recovers his property but often the person selling it is arrested and prosecuted for receiving stolen property and even the thief becomes vulnerable, especially if the fence attempts to make a case of his own innocence by claiming his ignorance of its stolen status by naming the thief. Thus, the bond between the legitimate owner and his property is increased commensurate with his ability to identify and locate it coupled with his proof of ownership.[21] Conversely, the bond between the thief and his fence is degraded commensurate with the risk

[19] Posse comitatus is a legal requirement compelling able-bodied men to assist a law enforcement officer when called upon. It is codified in the penal statutes of many states.
[20] This method is often referred to as "ubiquitous risk" in that anything that increases the risk of unpleasant outcomes decreases the behavior likely to lead to it. The greater the risk (surety of detection) the less likely the behavior will be repeated.
[21] Most often the only thing necessary to prove ownership is the fact that the legitimate owner has made a previous claim of theft and taken the legal steps to file a police report and seek recovery.

of being detected. Accordingly, anything that increases this risk becomes a force multiplier in its own right.

While law enforcement officers currently have the ability of searching stolen property databases for stolen property, allowing citizens to identify property on their own can dramatically enhance the likelihood of detection. This is occurring with increasing frequency as victims of thefts actively search websites like eBay, Craig's list, and other places where used goods are commonly sold, then report to police when they discover their own property for sale. A Web-based inventory of stolen property expands the reach of the citizen's ability to search without compromising any of the existing investigatory procedures. Simply listing stolen property with adequate identification (i.e. serial number) with the reporting agency and a means of contacting them provides the ability for collaboration between victims and law enforcement. Even unregulated yard sales and other places where stolen property is liquidated become vulnerable to detection and confiscation with the potential of prosecution and penalties.

With the advent of cell phones, mobile computing, and the like, applets would allow near instantaneous capabilities to check property before purchase. In a similar vein, many portable communications devices (cell phones and tablets, e.g.) contain software linked to a GPS capacity to locate them if lost or stolen. While a professional or experienced thief will know how to disable such protective measures, they remain a defense against casual theft.

Example #4: Under-Reported Drug Seizures

A drug courier associated with a notorious Mexican drug gang is intercepted with 500 kilos of drugs. During interrogation, the suspect refuses to identify his supplier or any pertinent information for fear that his life will be in danger from his criminal compatriots, a bond far stronger than any incentives police can provide for bargaining. A prison sentence for trafficking is the price of doing business—one for which he may well be rewarded—and the prison environment may include a gang that will protect him. If the individual is shown a press release

that credits him with only 400 kilos at the time of his arrest, the bond relationship changes. He knows he had 500 kilos, the police know he had 500 kilos, and more importantly, the narco-boss who trusted him with the shipment knows he had 500 kilos. The narco-boss will presumably assume that the trafficker for a personal profit diverted the 'missing' 100 kilos. Thus the trust relationship between the courier and the trafficker has been degraded, perhaps even destroyed.

The police have not exactly lied: the trafficker did indeed have 400 kilos. What the police have done is effectively enlisted the narco-boss as an unwitting confederate, a proxy who might inflict a harm from which the police themselves provide the best protection. Use of the under-reporting stratagem shifts the nature of the bond between the trafficker and the narco-boss to the point where a new bond is needed, a bond between the police and the trafficker, for the protection of the trafficker. With that shift, the interrogator has leverage to turn the trafficker into an informant.

While this may work as a tactic, it is unlikely that it will ever be accepted as a strategy given the admitted psychological influences that will inevitably be claimed 'forced' a suspect to confess. Variations of this method might be used in other manners, even if not as effective. Consider the same scenario multiplied by the hundreds of incidents in which it occurs. The only thing necessary to increase the risk is that police *not* report the exact amount of seizures, ever. This is well within the legalities and abilities of police agencies and creates a condition in which couriers are shielded when arrested because suppliers are never quite sure how much of the contraband was actually seized. This encourages couriers to become 'self-employed' by skimming drugs (unappealing but with no greater harm to the community) while simultaneously diminishing the trust between couriers and suppliers *in toto*.

Example #5: Prison/Street Gang Communications

Gang enforcement officers are well aware of the bond between prison gangs and street gangs. Gang leaders communicate strategy and decisions to subordinates in the community,

retaining effective control of the group's activities even though technically removed from society. Two high-profile cases that received extensive media coverage illustrate the case: Luis Felipe, known as King Blood, was kept in solitary confinement in New York because despite a murder conviction, he was directing not only gang activity of the Latin Kings, but violent retributions from inside the general prison population. On the West Coast, the Mexican Mafia issued a decree threatening death upon arrival in prison for any local gang members who even accidentally injured innocent Hispanic bystanders during shootings. Within two weeks gang-style shootings of houses and drive-by shootings had dropped by half. The fact that the Mexican Mafia had achieved a significant reduction in these crimes where law enforcement had failed—and without force— all but went without notice.

Like the narco-trafficker, a mutual trust—initially and ultimately based upon retributive force—binds the allegiance of free-world subordinates to incarcerated elders. We note, however, that members can internalize the rigid gang codes over time, eliminating the need for ongoing threats. The notion of bond disruption discussed below hinges not upon the initial violence, but upon the ultimate coercive force that lies in the Mexican Mafia example. Disrupting the bond relationship among gang members is as yet a hypothetical possibility, but technically possible. Though the gang communication routes involve both high- and low-tech means (cell phones, wall-tapping in codes, notes, messengers, corruption of prison guards and manipulation of non-gang inmates through favors and threats, etc.), increasingly robust surveillance measures make it possible to intercept the communications and break the codes. A series of false messages sent by law enforcement officials through a gang's communication networks would have the dual advantage of first, influencing any member who followed the directive, and second, arousing suspicion of even legitimate messages sent by the gangs. Countermeasures would have to be employed by gangs that would require additional security efforts and complicate communications forever after.

Example #6: Olfactory Isolations

Mob actions are in many ways the antithesis of criminal networks, where leaders are selected ad hoc rather than from proven merit and targets are more spontaneous than preplanned. In confrontational street actions—which are distinct from well-planned and organized protest activities—the mob is often incited by a small group of informal leaders with an agenda. In most cases these provocateurs are nearly immune from arrest while inciting a crowd because the force necessary to affect their arrest is sufficient to start the very riot that the police are attempting to avoid. Thus a dilemma is revealed in that allowing the provocateurs to continue is likely to result in a riot but arresting them is equally likely to result in the same outcome. In this case, the bonds between the provocateurs and the crowd are stronger (even if only temporarily) than those between the police and the crowd. Such bonds are ephemeral, usually forged by emotional reactions to a particular set of circumstances. The provocateur exploits the emotional state of the crowd by providing inflammatory statements and rationales, or falsely claiming to have observed police actions that did not occur.

Conventional riot control techniques and weapons may be justified to neutralize the provocateur, but can only be employed at great risk of inciting the very riot the police are attempting to avoid. Some technologies now provide an ability to simultaneously attack both the agitators and the bonds necessary to organize and oversee riotous behavior. One good example is with the use of a malodorant. Unlike conventional riot control agents that cause extreme discomfort with burning eyes, coughing, and painful breathing, malodorants simply smell bad—horribly bad! Malodorants can be delivered in the form of small projectiles (i.e. liquid-filled paint balls) that are painful but otherwise non-injurious. Once doused with a malodorant, however, the agitator has great difficulty in enduring the stench. More to the point, the natural protection measures for the people around him are to move upwind and farther away, thus degrading an ability to organize and incite the crowd. Furthermore, even brushing against the person contaminated is sufficient to transfer enough chemical to continue

the dispersal, much like the odor of a skunk. In this manner, the agitator becomes his own dispersal agent and for all intents and purposes, is the nonlethal equivalent of Typhoid Mary.[22]

As with any new strategy, there are many concerns that remain, not the least of which are legal and ethical concerns and public acceptance. Nevertheless, the principle of bond relationship targeting provides promising solutions for situations that are inherently difficult and dangerous and averse to conventional methods of deterrence. Traditional reverse sting operations have operated on the same principle as the options proposed above: when any on-street drug pusher, prostitute, or fence can be an undercover police agent, a criminal associate's ability to rely upon "trust" to complete a criminal transaction becomes seriously eroded.

Applying the bond disruption principle to networks and organizations will also carry a cost in terms of police personnel time and investment in equipment. The return for that investment lies in the greater impact across a wider population than just those who are arrested in a sting operation. The effects can be more long-lasting, extending the uncertainty and raising the cost of doing illegal business, any of which makes the criminal behavior less likely to reoccur.

[22] Mary Mallon became known as "Typhoid Mary," after it was determined that she was a healthy carrier of a deadly pathogen—typhoid fever. As used in this example, the agitator remains free but will continue to disperse the foul-smelling malodorant wherever he attempts to continue his illegal activities until he washes it off.

Intelligence, Management, and the Management of Intelligence

Bernard H. Levin

In any discussion of trust and transparency as it relates to intelligence, one would be remiss were one not to mention The National Commission on Terrorist Attacks upon the United States (Kean, 2004). Most readers are familiar with the findings of the Commission as they relate to intelligence. This paper will not re-plow that ground, but rather will focus mostly on classification proclivities and human frailties as we consider the future of intelligence.

I have experienced the joys and travails of various classification systems, from the Army Security Agency of yore to various local and state police departments, 3-letter agencies, and the private sector. In all of those domains, over the course of half a century, I have observed that a similar heuristic has prevailed -- when in doubt, classify. In the words of one of our colleagues, an experienced and well-respected police chief, "... they stamp that [‘law enforcement sensitive’] on everything including the lunch list." One might safely say the same of "for official use only," “restricted”, and similar phrases.

That colleague and I are by no means the first to note this. The Inspector General announced yet another review of over-classification at the Department of Defense (http://www.federaltimes.com/article/20120208/DEPARTMENTS01/202080305/IG-reviewing-overclassification-DoD). A couple of years ago, President Obama signed “The reducing over-classification act” (http://www.whitehouse.gov/blog/2010/10/07/president-signs-hr-553-reducing-over-classification-act). In 2004, the House of Representatives subcommittee on National Security, Emerging Threats and International Relations published, “Too many secrets: Over-classification as a barrier to critical information sharing” (http://www.fas.org/sgp/congress/2004/082404transcript.pdf). The earliest over-classification report that I have found is the report of the Coolidge Committee of 1956 (http://www.fas.org/sgp/library/moynihan/appg.html). Similar observations probably date to the dawn of classification. The above addresses only federal classification, but similar issues occur inside every law enforcement agency in the nation, all approximately 18,000 of them.

Sometimes the classification process manifests the absurd. For example, most of us probably have seen classified summaries of articles that have appeared in newspapers and without any analysis at all. That the source documents appeared in the open literature and are readily searchable on the Internet clearly does not bar classification of compilations. It merely makes the classification absurd. Sometimes even documents that have long been in the public realm have been retroactively classified, as if somehow all those in possession of them would disappear or no longer share them (e.g., Waxman, 2004).

Another range of absurdity is over-classification that results in merely sensitive information being labeled secret, top secret, or even higher. And a final range of absurdity is the duration of classification for items that may be embarrassing rather than threatening. Items half a century old yet still classified are not unheard of. Leonard (2011) provides us with an interesting case, to wit:

> Consider this strange case from earlier this year. On June 8, the National Security Agency, a top-secret government spy agency, heralded the "declassification" of a 200-year-old publication, translated from the original German, on cryptography. It turns out, however, as reported by Steven Aftergood of the Federation of American Scientists on his blog Secrecy News, that the 1809 study had long been publicly available and had even been digitized and published online through Google Books several years earlier. In fact, the 19th century study had not met the government's own standards for classification in the first place.

So, why is over-classification a problem for intelligence? Because classification is what silos are made of, what makes it difficult or impossible for us to grasp that "need to share" must trump "need to know" and even makes the job of analysts pointlessly difficult.

Transparency is an overarching force. It undermines the increasingly problem-prone nature of classification. We note when transparency takes big jumps, as with various Wikileaks exposés (e.g., Dishneau, 2012), but the social phenomenon that is the Internet, manifest via an evanescent set of social media, is an inexorable driving force for exposure. We push back the ocean, but the ocean will win. Rather than continuing to push back the ocean, our time would be better spent figuring out how we can use trust and transparency to make a safer and more secure nation. And world.

Some paths forward are reasonably obvious. Crowd sourcing of intelligence is familiar to many readers. So is net-centric information processing and sharing. A somewhat more radical approach might apply, to some extent at least -- open book management (Stack, 1992; Case, 1995). One might argue that the beginning of such an approach to intelligence is the Intellipedia (https://www.cia.gov/news-information/featured-story-archive/intellipedia-celebrates-third-anniversary.html). However, even if we were to defeat the forces of overclassification and we were to achieve total trust and transparency within the intelligence industry, we would still be faced with intelligence failures.

The Future: When Prophesy Fails . . . .

And, inevitably, it will. So, why will intelligence fail? There are many reasons, well beyond the usual complaints of classification/silos and inadequate/ insufficient collection/processing. It is worth re-reading Heuer's classic *Psychology of Intelligence Analysis* (1999). Heuer devotes five chapters to cognitive biases in intelligence work, although he does not happen to directly address those listed below. There are many more cognitive biases with the potential to distort or derail our intelligence efforts, e.g., see the "List of cognitive biases" page of Wikipedia.

1. Confirmation bias: We search for, select and remember information that supports our own perspectives and ignore, reject and forget information that conflicts with what we believe to be true. Confirmation bias is a strong effect and exists even when people are quite cognizant of the confirmation bias as having potential for distorting our conclusions. In the words of Klein (2011), “A full tabulation of all 17 questions showed that no group clearly out-stupids the others. They appear about equally stupid when faced with proper challenges to their position.”

2. Assumption of self-knowledge and self-prediction: Much of the evaluation and application of intelligence assumes we have a veridical or at least close-to-veridical picture of ourselves, our biases, our limitations, etc. However, available evidence makes

clear that the facts are otherwise, e.g., Wilson and Dunn (2004), and that there are significant differences in how self-knowledge works in, e.g., males and females (Boucher, 2011).

When it comes to self-prediction, we are not very good either. Koehler, White and John (2011), among many others, showed that our ability to predict our own behavior is heavily influenced by present conditions. If we have trouble predicting our own behavior, it follows that the use of intelligence to predict the behavior of others is unlikely to be any better and is probably even worse.

3. The rational man. The evidence that people are irrational and often maladaptive is overwhelming (e.g., Park & Kim, 2009; Reading, 2011; Baumeister & Lobbestael, 2011). Only the irrationally optimistic would assume collectors, analysts and consumers of intelligence to be otherwise.

On balance, given our intrinsic human handicaps and given in addition our insistence on hierarchical collection, processing and distribution of intelligence, it is amazing that we do as well as we do.

References

Baumeister, R., & Lobbestael, J. (2011). Emotions and antisocial behavior. *Journal of Forensic Psychiatry & Psychology, 22*(5), 635-642.

Boucher, H. C. (2011). Self-knowledge defenses to self-threats. *Journal of Research on Personality, 45*(2), 165–174.

Case, J. (1995). *Open-book management: The coming business revolution*. New York: HarperCollins.

Committee on Increasing National Resilience to Hazards and Disasters; Committee on Science, Engineering, and Public Policy; The National Academies. (2012). *Disaster resilience: A national imperative*. Washington DC: The National Academies

Dishneau, (2012, July 19). *Bradley Manning WikiLeaks case: Judge bars UN torture investigator from testifying*. HuffingtonPost, http://www.huffingtonpost.com/2012/07/19/bradley-manning-wikileaks_n_1687335.html

Heuer, R. J., Jr. (1999). *Psychology of intelligence analysis*. Langley, VA: Central Intelligence Agency.

Kean, T. H., Hamilton, L. H., et al. (2004). *The National Commission on Terrorist Attacks Upon the United States (The 9/11 Commission Report).* Washington, DC: Government Printing Office.

Klein, D. (2011). I was wrong, and so are you: A libertarian economist retracts a swipe at the left after discovering that our political leanings leave us more biased than we think. *The Atlantic*, December. http://www.theatlantic.com/magazine/archive/2011/12/i-was-wrong-and-so-are-you/8713/

Koehler, D. J., White, R. J. & John, L. K. (2011). Good intentions, optimistic self-predictions, and missed opportunities. *Social Psychological & Personality and Science, 2*(1), 90-96

Leonard, J. W. (2011). When secrecy gets out of hand. *Los Angeles Times*, 10 August. http://articles.latimes.com/2011/aug/10/opinion/la-oe-leonard-classified-information-20110810

Park, C., & Kim, H. (2009). The effect Of managerial overconfidence on leverage. *International Business & Economics Research Journal, 8*(12), 115-126.

Reading, A. (2011). Maladaptive behavior. *Meaningful Information, 1,* 135-142.

Stack, J. (1992). *The great game of business*. New York: Currency Doubleday.

Waxman, H. A. (2004). *Letter to the Honorable Donald Rumsfeld*. http://oversight-archive.waxman.house.gov/documents/20040629071638-64384.pdf

Wilson, T. D., & Dunn, E. W. (2004). Self-knowledge: Its limits, value, and potential for improvement. *Annual Review of Psychology, 55,* 493-518