

Updating Ethics Training—Policing Privacy Series: Managing Risk by Reducing Internal Litigation

By Thomas J. Martinelli, Adjunct Professor, Wayne State University, Detroit, Michigan; and Lawrence E. Shaw, Inspector, Florida Department of Law Enforcement, Investigations and Forensic Science Program, Tallahassee, Florida

Editor's note: This article is the fourth in a four-part series of privacy-related articles that appears in Police Chief magazine. The other articles are Thomas J. Martinelli and Joseph A. Schafer, "Updating Ethics Training-Policing Privacy Series: Taking Race out of the Perception Equation" (January 2011): 18–22; Thomas J. Martinelli, "Updating Ethics Training—Policing Privacy Series: Respecting Society's Evolving Privacy Expectations" (February 2011): 70–76; and Thomas J. Martinelli, "Updating Ethics Training—Policing Privacy Series: Noble Cause Corruption and Police Discretion" (March 2011): 60–62.

For years, ethics trainers have taught that all illegal behavior committed by a sworn member is unethical, but that not all unethical behavior is illegal. Still, policy noncompliance involving department investigations into members' private lives remains a dicey business. Invariably, department policies and procedures dictate that sworn members, and sometimes the nonsworn, must conduct themselves both on duty and off duty in accord with their organizations' expectations, citizen expectations, and ethical expectations, and not according to their own subjective privacy expectations. These are training issues that must be addressed at an academy level as well as during annual in-service training sessions.

Time and time again, officers accused of policy noncompliance for unethical behavior claim that they did not know that legal, but questionably moral, behavior would subject them to department discipline. The law enforcement profession demands the highest standards of duty and credibility in its members in order to accomplish its mission to protect and serve. This demand implies that the mission strictly adheres to the tenets of the profession and is carried out constitutionally, ethically, and legally. This philosophical template of professionalism is the cornerstone of productive community-policing relations. In the end, citizens are the stakeholders of policing services, and reducing department internal litigation, specifically unethical misconduct and privacy issues, is a mandatory organization-wide challenge.

Minimizing Litigation Is Managing Risk

Renowned lawman, lawyer, and annual IACP conference presenter Gordon Graham travels the country speaking about what managing risk entails in law enforcement circles.¹ He uses a succinct definition for risk management, describing it as "any activity that involves the evaluation or comparison of risks and the development, selection, and implementation of control measures that change, reduce, or eliminate the probability or the consequences of a harmful action."²

He has several risk management catch phrases applicable to law enforcement, such as "every identifiable risk is a manageable risk"; "the errors that he will make can be predicted from the errors he has made"; "things that go wrong in life are predictable, and predictable is preventable"; and "discipline is a form of training."

Graham understands policing and is adamant about supervisory proactive prevention as he lectures on the costly mistakes made by supervisors failing to adequately supervise. More times than not, department liability is the result of "a supervisor not behaving like a supervisor."³ Graham repeatedly emphasizes that running a police department is a systemic team effort, and when tragedies occur, management drops the supervisory ball and fails in its supervisory duties.

Examples of dropping the supervisory ball include failures to adequately educate sworn personnel regarding department expectations of both on-duty and off-duty conduct regarding unethical behavior. In police training circles, there is a distinct disconnect between training blocks regarding "coffee shop ethics" and gratuities and training blocks regarding officer privacy expectations. Specifically, there is a lack of attention and policy implementation to both off-duty activities and department-related information technology oversight.

Graham's wisdom regarding managing risk can be applied to the astronomical costs associated with internal litigation. These are the lawsuits employees engage in regarding labor law issues and discipline. To reduce liability, attorneys' fees, and hours spent in defense of lawsuits, law enforcement executives must repeatedly provide notice through training of department expectations for officer behavior. An agency can markedly reduce its liability from internal lawsuits (police officers supplementing their incomes by suing their departments) if designated blocks of training address organizational expectations pertaining to officer privacy issues. Training curriculums must explain what "keeping one's private life unsullied as an example to all" means in today's policing values. Minimizing internal lawsuits through notice reduces or eliminates costly litigation. In these times of having to do more with less, this is a cost-saving managerial tool that can provide only positive dividends for the future.

Others have mirrored Graham's definition regarding the organizational duties associated with departmental liability, which states that "risk management is a process that also includes basic managerial functions: planning, organizing, and leading, as well as controlling agency losses at a reasonable cost. It uses accepted managerial techniques in order to preserve the assets of an organization or entity."⁴ This systemic accountability demands department-wide training in the agency's expectations of officer behavior both on duty and off duty; policy implementation; vigilante supervision; and strict, swift, and certain discipline for policy noncompliance. Middle management buy-in for identifying potential risk, coupled with the use of early warning systems, is critical for success. Otherwise, organizational dysfunction results and can prove costly in civil court, win or lose.

When a member of a police department sues the department, the ultimate losers are the stakeholder citizens. This is an inexcusable cost that must be avoided. Failing to follow a risk management template for success, which must commence with a block of training comprehensively discussing systemic notice in training, can result in protracted internal litigation. What is worse is the problematic reality of having to reinstate a poor employee, with back pay, because a policy was void for vagueness or was inadequately addressed in training curriculums. Maintaining written records of training curricula and attendees is a strong defense against an officer's "I didn't know" defense.

Lastly, prioritizing potential risks is the key to successful risk management.⁵ There are plaintiff attorneys who make their livings suing departments regarding fatalities resulting from police shootings and pursuits. These are priorities that agencies historically have had to address due to their relative frequency and are generally forgiven by civil juries in wrongful death actions. Time and time again, the dangerousness of the job, the tragic situations officers confront on a daily basis, and the split-second decision-making processes officers have to engage in cause juries to side with police departments. These lawsuits, though a part of the public service professions, must be minimized at all costs.

Civil trials for internal litigation involving unethical officer behavior and privacy issues may find that taxpayers are not as forgiving of the police in their jury verdicts as the disciplined officers would like them to be. Taxpayers are the clientele of the police department, and knowledge of their officers' off-duty promiscuity, on-duty derelictions, and sexual trysts may not result in their blind-faith forgiveness. Agencies have a duty in assessing their risk management priorities to minimize or alleviate the potential for all types of costly internal litigation.

Privacy Expectations and Off-Duty Sexual Trysts

Labor law literature is rife with examples of officers involved in off-duty sexual trysts. For years, police ethics trainers have referred to a wrongful discharge lawsuit wherein an officer involved his wife, his 18-year-old sister-in-law, his scout car partner, and tangentially, his entire department in a sex scandal that resulted in his termination.⁶

Rumors were rampant throughout the department that the 18-year-old was engaged in nefarious relations with numerous officers. The woman's parents complained to the chief, the mayor, and eventually to the media. Once the internal investigation was finalized, it was discovered the officer in question solely orchestrated sexual trysts with his scout car partner and his wife in order to seduce his 18-year-old sister-in-law.

The key to this case was the court's conclusion that the terminated officer knew, or should have known, that his legal but unethical off-duty behavior could cost him his job. His actions constituted unbecoming conduct, brought discredit to the entire department, and gave the citizenry, through extended media coverage, the perception that their police officers spent more time pursuing sex than protecting the streets.

In upholding the officer's termination, the court rejected the defense that the officer did not know his off-duty unethical behavior would deprive him of his job and police pension. In fact, the court used the IACP Code of Ethics as the template of notice, stating that the officer knew he was to "keep his private life unsullied as an example to all" if he wished to be a part of this noble profession. In a paramilitary structured organization, such unethical behavior is dysfunctional and tarnishes the good image of the agency in the public's eye.

Further, thousands of taxpayer dollars were used by the department to defend the lawsuit. In this case, one can conclude that the agency's termination process took many hours to investigate; litigate (in department labor hearings); and eventually defend in civil court. These internal law enforcement lawsuits are counterproductive, inefficient, and require significant time and money. In the end, the citizens the agency is tasked to serve are the losing faction.

Internal litigation is a management risk that is predictable, preventable, and can usually be avoided, or minimized, with adequate training, policy implementation, and middle management buy-in. There must be an organizational understanding, between rank and file, as to privacy expectations of the department and written policies supporting that understanding. Organizational training mandates limiting employee privacy expectations, coupled with department policy compliance measures, are the keys to successfully diminishing internal lawsuits.

Information Technology, Privacy Expectations, and Internal Litigation

In this age of information technology (IT), there will always be the organizational challenges of expediting law enforcement services through technological means and employee privacy expectations associated with these IT tools. One could argue it is a dereliction of duty for a law enforcement agency to not embrace this modern age of technology in order to better serve its constituents. But as the tools of the trade become more sophisticated, the rules of law associated with the use or abuse of those tools becomes more challenging.

Police administrators must employ a comprehensive IT privacy policy that instructs all sworn personnel using agency-supplied technological equipment that this equipment is to be used solely for police matters; that all communications will be randomly audited for work-related purposes; and that there exists no employee expectation of privacy for the use of such technological equipment. In this way, misconduct allegations are reduced, internal investigations are minimized, discipline in this regard is practically nonexistent, and plaintiff lawyers will have less causes of action to sue departments.

Organized policy implementation reduces departmental risk, but poorly drafted or vague policies have forever provided internal litigation headaches in policing. The wording in the policies themselves, coupled with assumptions, implications, and a blind faith that employees will always do what is morally right, have cost agencies time, money, and sometimes a drop in morale with increased employee cynicism. The "supervisory logic of good faith"⁷ presumes that subordinates will comply with policies and procedures and can police themselves in regard to policy compliance issues. As Graham said at IACP 2009 in Denver, "Show me a tragedy in law enforcement—and almost without exception (and there are some exceptions) I will show you the fingerprints of a supervisor not behaving like a supervisor."⁸ The U.S. Supreme Court recently had to adjudicate a poorly worded and poorly implemented department IT policy in deciding Fourth Amendment privacy issues.

In the case *City of Ontario, California, et al. v. Quon*, the Ontario, California, police department provided its special weapons and tactics (SWAT) team members with alphanumeric pagers, as the court put it, "in order to help the SWAT team mobilize and respond to emergency situations."⁹ The agency purchased 25,000 text characters (letters and spaces) a month for each member's pager, and the text messages from the pagers were subject to the agency's computer policy. That policy stated that the city reserves the right to monitor and log all network activity including e-mail and Internet use, with or without notice, and that "users should have no expectation of privacy or confidentiality when using these resources."¹⁰ Subsequent training at a staff meeting for the SWAT team and a memo from the chief further stressed that the texts sent on the SWAT pagers were considered departmental e-mail and were subject to random audits. The plaintiff, a sergeant on the SWAT team, fully acknowledged the computer policy, the relevance of the pager's use with that policy, and the 25,000 character limit per month.

Despite this departmental policy of notice and officer acknowledgement, the sergeant filed a Fourth Amendment privacy rights violation suit against his employer after he was disciplined for his improper use of the SWAT pager.

The sergeant's discipline resulted from an internal affairs investigation regarding his on-duty use of the pager for personal matters. The chief audited the team's text messages to see if the department needed to purchase more monthly characters. The internal affairs investigation concluded that the plaintiff, in the month of August alone, sent or received 400 personal messages while on duty, which had nothing to do with the duties associated with the SWAT team. His record for one day at work was 80 text messages, and his daily average for sent or received personal messages was 25 texts. The investigation also discovered that some of the on-duty personal messages were sexually explicit in nature. After the sergeant was disciplined, he filed his privacy violations lawsuit.

Despite the presence of a written computer policy; further training on that policy; and a memo from the chief stating that all departmental networking, including the text messages from the SWAT pagers, were subject to random audits, the plaintiff argued his privacy expectations to the on-duty texts were violated. He argued that a subsequent verbal agreement between the team and its lieutenant nullified the computer policy, at least in regard to the SWAT pagers. The lieutenant assured the team members no one from the agency would audit the team's text messages as long as they personally reimbursed the city for all monthly overages exceeding the allotted 25,000 texts per month, per pager. The court ruled in favor of the department.

Though the U.S. Supreme Court's analysis is long and arduous, reading between the lines facilitates a swifter conclusion. The court concluded that the plaintiff had a limited expectation of privacy, if any at all, and that the search was reasonable under the circumstances and under any Fourth Amendment application.

The majority relied heavily on the facts of the case. The plaintiff was a supervisor. He knew the policies and the agency's purpose behind those policies. He was on a special tactical team, held to higher standards than street-level supervisors due to the dangerous nature and duties of a SWAT team. The purpose behind the acquisition of the pagers was to facilitate work-related communications between the team members.

The court concluded that the plaintiff was a veteran officer and knew, or should have known, that department-issued communication technologies are many times subject to (1) review for performance evaluations; (2) reasonable Freedom of Information Act requests by citizens or the media; and (3) the lenient discovery rules used in civil lawsuits, especially lawsuits in which SWAT team members most likely would be involved. For these operational realities, coupled with knowledge and notice of the computer policy, the court rejected the plaintiff's expectation of privacy argument.

In this discussion of managing risk by reducing internal litigation, how did such a case, as costly as it was to the taxpayers of that community, ascend to the U.S. Supreme Court? On its face, the sergeant did not seem to have much of a legal leg to stand on from the outset. This is where poor policy drafting and poor policy implementation can cost an agency the multitude of hours and attorney fees associated with such internal litigation.

First, as previously mentioned, the plaintiff hung his privacy expectations argument on the lieutenant's subsequent verbal assertions that the department would not audit the SWAT team's text messages as long as the team members paid for their own overages. The lieutenant lacked the authority and the policy-making powers to circumvent a written departmental policy, and the court recognized that. This is an issue that must be addressed in supervisory training circles. Verbal, additional, or implied changes to written departmental policies cloud misconduct

issues and disciplinary procedures and may fail in labor law hearings.

Secondly, the computer policy and subsequent text message training for the SWAT team never specifically addressed personal usage of the pagers, whether used on duty or off duty, and the discipline to be meted out for any policy noncompliance. It seems that as long as the team members did not exceed the 25,000 characters allotted, personal use, both on and off duty, was permissible. But had the plaintiff never exceeded his monthly characters, would the chief have been justified in ordering an audit of the text messages? The answer is yes; all random audits in policing have a special needs purpose in the professional administration of a department, and employee privacy should never be an issue.

Why, then, was a costly jury trial held to determine the chief's intent in ordering and auditing the team's text messages? The departmental technology policies themselves never mentioned that the chief, the internal affairs department, or anyone with the authority to audit those messages had to rely on a Fourth Amendment exception to read those employee messages. Random audits in the workplace are just that: random, with no need for reasonable suspicion, probable cause, or allegations of misconduct. A random audit policy gives administrators carte blanche authority to audit all technological communication associated with department-issued equipment. Random audits of in-car videos, in-car lien communications, and Internet audit trails are specifically intended to deter employee abuses. The philosophy behind random audit policies is to deter any employee temptations to abuse their access to the specific technology available. This should have been explicitly written in the computer policy in order to deter the very behavior the plaintiff engaged in: his personal texting on duty.

A time-consuming, costly jury trial was held to decide the chief's intent in auditing the team's text messages. Written random audit policies alleviate any causes of action for bad faith, illegal searches, or maliciousness on the part of a chief of police or the internal affairs unit.

Though the jury ruled in favor of the chief, concluding that his audit had a legitimate, work-related purpose, thousands of taxpayer dollars were spent on this trial, as well as the monies spent for the appellate case and eventual U.S. Supreme Court proceedings. Focused policy verbiage regarding the agency's intent to conduct random audits, coupled with frequent random audits and appropriate disciplinary measures, most likely would have deterred the sergeant's abuse of the pager and eliminated any internal litigation paid for by taxpayer dollars. Notice, through training curricula, of how policies will be implemented and supervised is the key to limiting costly litigation.

Taxpayers are the stakeholders in the police business. The majority of justices, in this case, questioned what society accepts as proper behavior in regard to technological privacy expectations in the workplace. The answer is most likely that private citizens have little expectation of privacy at the workplace regarding their employer-issued desktops, laptops, and networking tools. In order to decrease extraneous Internet surfing, following sporting events, and excessive personal e-mailing during work hours, private employers issue directives informing their employees that audit trails are randomly conducted to prevent such wasteful uses of their work time and their computers.

In his concurrence with the majority, Justice Antonin Scalia reiterated his position from a previous employment privacy case wherein he wrote "that government searches to retrieve work-related materials or to investigate violations of workplace rules—searches of the sort that are regarded as reasonable and normal in the private-employer context—do not violate the . . . Amendment."¹¹

The laws of privacy continue to evolve in criminal courts and in labor law courts. As technological advances continue to enhance police services, agencies must revisit their own policies and procedures related to informational technology and employee privacy expectations. Only through training programs can department notice be established regarding policy implementation. Additionally, comprehensive ethics training curriculums must emphasize the sanctity of privacy issues in policing, both as applied to target citizen investigations and to internal affairs issues. Internal lawsuits are counterproductive and costly in relation to the overall agency mission to protect and serve. ■

Thomas J. Martinelli, MS, JD, is a practicing attorney and an independent training consultant for both the Institute for Intergovernmental Research, Tallahassee, Florida, and Michigan State University's Intelligence Toolbox Program, East Lansing, Michigan. He trains in police ethics and liability and intelligence-led policing, specifically addressing privacy issues. He is a member of the IACP Police Image and Ethics Committee.

Lawrence E. Shaw coordinates the flow of criminal information and intelligence between federal, state, and local law enforcement agencies, using automated information systems. He has more than 23 years of diversified law enforcement and criminal investigative experience and seven years of emergency response experience.

Notes:

¹To read more about Gordon Graham's advice for managing risk, visit <http://www.Lexipol.com>.

²Gordon Graham, "Risk Management in Policing" (lecture, Macomb Community College, Clinton Township, Michigan, October 2004).

³Gordon Graham, "Line Officer Training: Accountability for Supervisors: A Primer on Managing Risk" (presentation, IACP 2009, Denver, Colo., October 5, 2009).

⁴Darrell L. Ross, *Civil Liability in Criminal Justice* (Cincinnati, Ohio: Anderson Publishing, 2003), 73.

⁵Kim Mays, "Definitions: Risk Management," *IT Business Edge*, last modified April 1, 2009, <http://www.itbusinessedge.com/cm/docs/DOC-1312> (accessed January 31, 2011).

⁶*Fabio v. Civil Service Commission of the City of Philadelphia*, 414 A2d 82 (Pa. 1980).

⁷John Crank and Michael Caldero, *Police Ethics: The Corruption of Noble Cause* (Cincinnati, Ohio: Anderson Publishing, 2010), 47.

⁸Gordon Graham, "Line Officer Training: Accountability for Supervisors: A Primer on Managing Risk."

⁹*City of Ontario, California, et al. v. Jeff Quon et al.*, 560 U.S. ____ (2010), 6, <http://www.supremecourt.gov/opinions/09pdf/08-1332.pdf> (accessed January 31, 2011).

¹⁰Bill Mears, "Supreme Court to Hear Texting Privacy Case," *CNN*, April 19, 2010, http://articles.cnn.com/2010-04-19/justice/scotus.text.messaging_1_jeff-quon-text-messaging-arch-wireless?_s=PM:CRIME (accessed January 31, 2011).

¹¹*Quon*, 560 U.S. ____2–3, quoting Scalia's concurrence in *O'Connor v. Ortega*, 480 U.S. 709, 732 (1987).

Please cite as:

Thomas J. Martinelli and Lawrence E. Shaw, "Updating Ethics Training-Policing Privacy Series: Managing Risk by Reducing Internal Litigation," *The Police Chief* 78 (April 2011): 112–118.