The Bill Blackwood
Law Enforcement Management Institute of Texas

Information Sharing

A Leadership White Paper
Submitted in Partial Fulfillment
Required for Graduation from the
Leadership Command College

By
Joe Roy Williams Jr

Stafford Police Department
Stafford, Texas
September 2019

ABSTRACT

For far too long the law enforcement community has been hindered and divided by a decline in relationship building between local, state, and federal agencies. All law enforcement agencies follow a mission statement or embrace a set of core values, including honor, commitment, integrity, and community service. These agencies should also aim to express those same values in relation to other law enforcement agencies. Officers have been too comfortable in their adoption of the “them and us” mind-set, reflecting the idea of no interdependent law enforcement personnel and practices.

Law enforcement agencies must work to end this mind-set and move in a new direction of partnership with each other, recognizing the benefits of mutual understanding and respect. Regardless of the size of an agency, among its goals for agency-community connection should also be service to fellow law enforcement officers. Using examples from Texas, this paper aims to dispel those “them and us” perceptions and introduce the interdependent policies and practices that would greatly benefit law enforcement agencies in the state and across the nation.

TABLE OF CONTENTS

INTRODUCTION

In Texas, the law enforcement community is among the largest communities with its 1,913 agencies – the most of any state. These agencies employ 59,219 sworn police officers and are constantly adding to that number. In the multiple Texas law enforcement agencies, a small number employ a large roster of reserve officers, and larger agencies encompass a vast number of full-time officers (Reaves, 2011).

All agencies are part of this great family of blue. However, the fact that different law enforcement agencies are hesitant to share information and jurisdictional territory with one another is a key issue. Such resistance may have contributed to preventable tragedies, in such with the US Border Patrol agents had intercept a man when he entered the United States illegally from Mexico. Unaware that he was wanted by the Federal Bureau of Investigation (FBI) for three murders, the Border Patrol deported him. The man returned to the United States, ultimately murdering several more before being caught. (Robert Mitchell-Computerworld 2008)

Robert L. Mitchell (2008) laments the lack of communication between the Border Patrol and the FBI may have contributed to these deaths. He also notes that, in North Carolina, “a team of investigators worked for 20 years to bring down an international drug-trafficking organization” (para. 2). Had the team had access to other law enforcement databases, the case might have been closed sooner! The Metropolitan Transit Police Department also deals with the frustrations of not being able to share information with surrounding law enforcement agencies. Bureaucracy is the highest hurdle. Specifically, if an officer makes an arrest, that officer must complete three reports. An initial report goes to the Metro reporting system to verify that the officer was dispatched to the call for service. A second report is submitted to the Houston Police Department's data system because an arrest was made in the city. The third report is made to the Harris County Sheriff's Department (via the Harris County reporting system) to book the arrestee into jail (National Criminal Justice Association Initiative, 2004).

A lack of information sharing on cross-border, local, and state levels causes one type of emergency response delay and citizen threat, but a lack of information sharing on national and international levels, such as observed with the September 11, 2001 terrorist attacks on the World Trade Center and the Pentagon, reveals the extent of danger to shake the national infrastructure and citizenry. Not only did this event immediately obtain media coverage, that coverage highlighted how the nation was shook to the core. This event impacted the lives of many people living both in and outside of America. A nation that was once perceived as one of the strongest suddenly began to cast doubt on that claim. In a manner of minutes that sense of security was immediately taken away. That day will never be forgotten and many will continue to live in fear or have serious concerns when flying internationally or domestically.

Midtown Manhattan was devastated by the initial crash and the subsequent collapse of the World Trade Center. The Pentagon was severely damaged by a direct hit from a jet flying at top speed. Farmland in western Pennsylvania was rendered useless by the crash of the third aircraft that did not reach its intended target. This horrific event did not discriminate on the lives that it took that day, no person or social class was protected. There were literally thousands innocent of lives taken, and at what cost? If intelligence agencies were working together, it is very possible that this tragedy could have been detected and/or avoided.

In the traumatic weeks after the attacks, reports were compiled, and it became clear that lack of communication was the common denominator in the tragedy. The three terrorist plots took advantage of flaws in the U.S. information system and thwarted all levels of law enforcement, even in the nation that led the world in technology and intelligence gathering (Mitchell, 2008). Information sharing, however, was (and still is) a problem (Rutledge & Inserra, 2017). The FBI, the National Security Agency, and the Central Intelligence Agency did not pass intercepted information about a credible terrorist threat on to state or district police departments, and those police departments did not pass information on to local authorities. This communication breakdown and “intelligence failure,” as it was labeled by former FBI special agent Mark Rossini, might have been prevented by the sharing of pertinent information among law enforcement agencies at all levels (Stein, 2015, p. 2).

While the need to improve information sharing among the many levels of law enforcement—the FBI, the Drug Enforcement Agency, and the Department of Justice—was recognized, or at least alluded to, previously (Schneier, 2009; Szerlag, 2013), the events of 9/11 brought to the fore the need for information sharing among law enforcement agencies. The 9/11 Commission, formed in 2002 to root out the causes of the attacks, ultimately acknowledged intelligence failures existing before 2001 and concluded that the nation was “not well served” by a CIA and an FBI that did not share information (9/11 Commission, 2004). Another classified report added to the critique, suggesting that tensions between intelligence and criminal investigations—“inter-agency rivalries and turf battles”—not just legal barriers, “allowed” terrorists to carry out their heinous acts (Grewe, 2004; Schneier, 2009, p. 1).

Even with the catalyst of the attacks, the official and private statements of the 9/11 commission members, and a presidential mandate for better information sharing, more than one decade after the attacks, Assistant Director of Intelligence for the FBI Eric Velez-Villar spoke to the House Homeland Security Committee about the still-existing need for “fusion centers” to coordinate and integrate intelligence dissemination toward “maximizing our ability to detect, prevent, investigate, and respond to criminal and terrorist activity” (Velez-Villar, 2012, p. 3).

This paper concurs with concerns about information sharing and local, state, and national security. Further, it asserts that law enforcement agencies should utilize the same records management system. A shared system of recordkeeping, easily accessed and updated by all agencies, will create a closer law enforcement community, increase the safety of societies, and provide better service to citizens.

POSITION

A shared records management system can create strong relationships and foster mutual trust among police agencies. Sanders (2010) notes that individual law enforcement agents are on one team; to be truly effective they must be able to share data and intelligence securely across jurisdictions. In their examination of ways to improve law enforcement information sharing, John S. Hollywood and Zev Winkelman (2015) concluded that “a multilayer framework for sharing law enforcement information should be created. . . . This framework should include a master data model describing how to share data elements used across multiple standards, software development kits for building and implementing standards, and expanded testing and certification. It should also include critical interfaces that have not yet been captured in existing or planned standards" (p. 2).

Indeed, history offers a reminder that, for example, when a military force is well prepared for battle, the chance of defeating the enemy increases. Such preparation is often overlooked in discussions of law enforcement. Equally underestimated is the level of communication among targets of law enforcement, such as gangs. Local gangs such as the Bloods, Crips, and North Side Boys, has a distinctive way of communicating with each other. The high level of their communication includes hand gestures, lettering or graffiti in which members only could interpret what is being said.

Linked law enforcement agencies can create a community of networking with one common goal for law enforcement: connectedness. Connectedness can be examined across varying types of crime pursued by law enforcement. For example, links among cybercrimes, sex crimes, identity theft, and drug investigations can, at times, force agencies to work closely together and share general knowledge (Trend Micro, 2014). Assigning officers or agents from the larger agencies such as on the federal, state level to work closely with personnel from the smaller agencies can create a stronger, more productive, and lasting relationship (Stuart & Taylor, 2017).

Cross-training is also another way to allow agencies to work closely together. Most often used for police officers and firefighters, cross-training allows a city to, for example, train workers in both agencies as paramedics (rather than as basic life support providers), creating a single public safety department (Garrett, 2008; Romney, 2013). Law Enforcement agencies that partner for cross training immediately reap benefits from the interaction. The officers, or agents conduct fire range exercises, completing misdemeanor/felony traffic stops, and area search operations become familiar with how other agencies conduct training exercises. Completing and exercise like this, it will assist both agencies just in case an incident arises which may call for both organizations to work together.

Cross-training can also benefit in undercover operations. Operations within certain jurisdictions would connect officers already familiar with each other through combined training. Ultimately, cross-trained law enforcement agencies can tear down the walls of separation that have been preventing the creation of a true public safety entity (Zukewich, 2004).

Drug use was treated as a small-town issue several years ago, however, it is now a larger problem that affects law enforcement at all levels. All agencies are depending on each other for information on the subject. Sharing information can lead to more arrests and can reinforce the closeness between the two entities and justify extra efforts.

Joint task forces, such as the Special Crimes Unit, Special Weapons and Tactics, and the Crisis Intervention Team, are formed to combat issues within those respective jurisdictions. State and local task force are very beneficial at fighting complex issues and being able to facilitate the needed resources. By the time these teams are called upon, information has already been shared between the agencies, facilitating multiple arrests. Not just one agency can indulge in a moment of chest beating but the entirety of law enforcement can celebrate. Several of those moments occurred simultaneously in New Jersey and Virginia in 2010 when 9 individuals were indicted for trafficking guns between the two states. The arrests and indictments resulted from a historic partnership involving the New Jersey State Police, the U.S. Bureau of Tobacco, Firearms, and Explosives Task Force, and the Division of Criminal Justice Gangs and Organized Crime Bureau (“Nine Indicted on Gun Trafficking and Weapons Charges,” 2010).

Public safety dispatchers are a crucial part of information sharing among the teams. They are the first line of communications, constantly receiving and disseminating all types of information fed into their call centers (Bune, 2014). Other important factors are those agencies that schedule monthly meetings, training, and updates for employees; they also assist in building stronger relationships between each agency.

The lynchpin for all of this connectedness is a shared cloud computing system. “The FBI’s Criminal Justice Information Services defines the cloud as a model that provides on-demand access to a shared pool of computing resources. It is much like having extra computing power or a large hard drive in another place where data may be stored and/or processed. Through the cloud, data, images, video files, and more can be securely stored, processed, and analyzed in a fully managed remote environment” (U.S. Department of Justice, 2016). With three-quarters of the nation’s fourteen thousand local law enforcement agencies having twenty-five or fewer sworn officers, and nearly half with fewer than ten officers, cloud computing is an important means of connection among officers in smaller agencies and to larger public safety hubs.

In practical application, the cloud saves an officer valuable time. A patrol officer who encounters a subject on the street has no way to immediately confirm the subject’s legal history. The officer depends on the dispatcher to conduct a criminal history check, a process that takes more than mere minutes. If the dispatcher ultimately learns that the subject has a confirmed criminal history, the last arresting agency is contacted. This entire process, from initial subject contact to notification of previous arresting agency may take up to ten minutes. The cloud system can cut this time to minutes, and allow the officer to conduct the search independently. The officer could access the cloud to obtain pertinent information on the subject, such as a photo, past addresses, criminal history, gang affiliations, and whether the subject is wanted in any ongoing investigations by surrounding agencies. For an officer working the graveyard shift, in which staffing of dispatchers are few in number during the overnight shift. The benefits of such access would be immeasurable, as the cloud would immediately alert the other agency looking for the suspect—a process that previously would have had to wait until the daylight hours (Young, 2013).

The Metropolitan Transit Police Department is responsible for the safety of public transportation in the city of Houston, even though the bus and rail lines travel into the jurisdictions of multiple safety agencies. Metropolitan Transit has placed bus shelters in all the outlying areas served by busses, and, although the transit company is responsible for the shelters, at times other local safety agencies must monitor the areas.

The city of Bellaire has several Metropolitan Transit bus shelters and park-and-ride lots within city limits. Although the transit company is responsible for these locations, sometimes Bellaire police are dispatched to the property for various disturbances. If Bellaire officers check a stopped subject in their database, the subject may appear as warrantless. However, that same subject may have multiple criminal trespassing warnings in the Metropolitan Transit Police Department database, prohibiting the subject from entering any transit properties. Instead, checked against an unlinked database, the person would be free from detention because no warrants appear in that system. Via the cloud system, that subject would be arrested because the warrant information would be the same across the board. Such a system creates a win-win circumstance for all law enforcement agencies.

The Oakland, California, Police Department is piloting a cloud storage program with a service that meets FBI's stringent security standards for data sharing on the Criminal Justice Information System (Newcombe, 2014). Oakland has invested in additional features, as well, including a digital signature used to authenticate videos in the context of criminal investigations. Officers at any time would have the ability to review video and audio footage from other agencies. Officers having the capabilities to conduct searches could and should assist in their investigations, which the aim is to increase the arrest. This also provides officers the ability to view footage that other agencies may have obtained.

The cloud will also allow analysts and officers to search for crime trends in certain geographic areas. Law enforcement officers would be able to access the cloud system when confronting subjects from other cities. Officers would be made immediately aware if the stopped person had a history of criminal activity, reading notes entered in real time by other linked agencies and adding to the discussion for other agents. Simple notes are of more assistance than might be assumed when officers are trying to piece together information when interviewing subjects (Marshall, 2011).

Most law enforcement organizations already have the information technology infrastructure needed to access the cloud system. The fundamental requirements are stable and secure for applications involving the downloading of information (Newcombe, 2014). Software migration and upgrades strain personnel due to the time and effort it takes to become accustomed to new platforms. If possible, agencies should attempt to utilize platforms that are similar to the ones that are currently used by the organization. If this is done it will greatly reduce frustrations and the amount of time spent on the learning curve.

The cost of the cloud system is another great benefit. Agencies across the nation have constraints on their yearly budgets and are constantly looking for ways to spend wisely. The cloud system costs are based only on an agency’s usage, fairly closely tied to agency size would cost the participating agency only for their usage. This approach would make such an endeavor easier to obtain for smaller and even large agencies. Oppose to having a set fee like so many others, the fee would be determined by usage.

The Houston Police Department 2016 annual budget was estimated to be $854 million. The Harris County Sheriff’s Department annual budget for the same year was estimated at $456 million. A smaller city agency, the Stafford Police Department, had an annual 2016 budget of $8 million (City of Stafford, Texas, 2017), much lower than the expenditures of the metropolitan and county departments. Regardless of budget, however, all three agencies could afford to use a cloud system, charged based on their budgets that would make information sharable across their jurisdictions, ultimately keeping citizens safer.

When as agency makes a capital investment in infrastructure and fixed storage capacity, it can often be asked how much capacity in the cloud system is needed. With the cloud system agencies only pay for what is needed. If an agency needs more storage or usage the cloud system allows the agency to scale up or down within minutes. Again, ultimately the goal is to make pertinent information available to all law enforcement personnel, and a cloud system seems to be most promising in accessibility and affordability.

COUNTERARGUMENTS

Although there are many benefits to information sharing, some agencies have some reservations about such collaboration. For many years law enforcement agencies across the nation have struggled with the “us versus them” mind-set—not in relation to criminals but in relation to each other, with the idea that law enforcement agencies compete among themselves for public support, funding, and political recognition (Smith, n.d.). That stigma rings true today; agencies might work closely together but not know one single officer from a neighboring agency.

Without report sharing within law enforcement, a Metropolitan officer can accumulate overtime by having to do the research and information gathering that could be done via an integrated cloud system. Yes, the officer benefits to a certain degree, but over time that overtime budget continues to increase, and such budgeting may raise scrutiny when the underlying cause is report/information sharing. Further, that overtime does not necessarily translated into more productivity. Officers completing multiple reports for one incident or arrest will at times will have an officer looking for lesser solution rather than making an arrest.

Barriers to information sharing must stop for all law enforcement agencies to be successful and effective. Agencies’ hesitation to share information and work closely with other agencies is understandable, i.e. officers’ unjustified acts such as Use of Force on citizens, conduct unbecoming, and unlawful arrest just to mention a few (Wyllie, 2009).

The Los Angeles Police Department (LAPD) is a great agency, however, a few high-profile cases in which questionable police decisions were made, such as O. J. Simpsons arrest in 1994 and the 1991 Rodney King beating, have blackened the department’s eye. Racism within the department is a concern for other agencies who are not wanting to share information or form a partnership with the LAPD (Malnic & Ferrell, 1994).

At the New York Police Department (NYPD) in 2016, Deputy Chief Michael Harrington was charged with corruption (Jackman, 2016). In Killeen, Texas, in June 2016, former officer Christopher Morris was indicted for sexual assault and official oppression (Associated Press, 2016). In that same month, Philadelphia police officer Thomas Vitanovitz was charged with extortion of a suspected drug dealer (Sasko, 2016).

Over the past 5 years the Houston Police Department has had officers charged with a wide range of crimes. Officer Julissa Guzman was charged with tampering with evidence related to narcotics, and Officer Noe Juarez was sentenced to thirty years in prison on federal drug charges (Kadifa, 2017; Murphy, 2015). Juarez was a veteran officer in the department, assigned to the traffic division. Juarez also had links to the Los Zetas drug cartel, supplying vehicles, body armor, and semiautomatic weapons to the cartel (Murphy, 2015).

The officers kidnapped a drug suspect to prevent him from testifying in federal court. The arrests came after a 2-year joint investigation of the FBI and the Philadelphia Police Department Internal Affairs unit. Field units like this one provide one of the greatest challenges to a cloud information system; no agency would want to share information with this team (Assefa, 2014).

A similar circumstance plagues the Baltimore Police Department, where officers were charged in the death of Freddie Gray on May 1, 2015 (Bertrand, 2015).The New Orleans Police Department has had the highest number of officers arrested in the past several years (Jackman, 2016). Forty-four officers have been charged, including some arrested during the aftermath Hurricane Katrina. It is understandable that so-called clean running agencies would not want to collaborate with agencies engaged in these types of behaviors. The Department of Justice has investigated many of these agencies for their illegal activities, but it is clear that police are not committing crimes anywhere near the level of civilian criminal activity. Law Enforcement agencies are understanding that the perception of officers are not positive in some instances. However law enforcement agencies are taking a proactive approach in re-enforcing policy, procedures to hold officers accountable for their actions.

Aside from agencies' security concerns in sharing information via the cloud is the concern with the technology itself. Many police departments have strong information technology firewalls to protect the sensitive text, audio, and video information stored in their databases. Hackers at times pose a threat to the law enforcement community, cybercrimes, has an agency at times feeling powerless. Agencies have found out the hackers age could be as young as elementary students. Video games at times can be an introductory to children into the world cybercrimes. Criminal hackers continue to pose an immediate risk in various aspects of the virtual world. Although law enforcement is trying to combat the issue it has proven to be a very daunting task.

Cybercrime is so prevalent largely because it is so lucrative. The number of compromises, record disclosures, commissions of bank fraud, and identity thefts in the number in the thousands. Apple has created watches, phones, and computers on which users can easily communicate with persons on the other side of the world just by pushing a button. All of which are ideal situations for hackers to exploit. The number of hacking incidents, combined with the fact that law enforcement officials are stretched thin in efforts to address cybercrime, make locating and prosecuting criminal hackers difficult (Shinder, 2011).

Hackers are usually arrested on a conspiracy charge, which carries a maximum penalty of five years in prison and a $250.00 fine. Hackers rarely serve the maximum sentences because they often plead guilty to receive more lenient sentences. Law enforcement suggests that parents should talk to their children about illegal computer activity such as illegal downloading of music or movies (Petty, 2011). It seems that parents could play a very important role in directing children’s lives away from cybercrime, although, in most cases, those who become hackers do not view these activities as crimes (“Cybercrime and Punishment,” 2014).

Hope still exists for a secure cloud information system, however, as education agencies have put in place programs to make children aware of the ethics of computing (Sicart, 2009). Law enforcement agencies have also designed a set of steps for combatting hackers prior to arrest and as part of the plea agreement (Forbes

Technology Council, 2018). Dealing with the issue before it happens and continuing to address it after it occurs allows law enforcement agencies to have a better understanding how the attack is conducted and give instructions on how to address vulnerabilities. Such public-private tools and tactics could extend to information shared among agencies via a cloud system.

Many law enforcement agencies have begun taking proactive approaches and informing both their residential as well as their business community about the cybercrime and ways in which he can offer a level of protection. Businesses are also being advised to spend the capitol to increase the security of employees' data and ramp up digital education to minimize ransomware attacks. This information is detailed, specific, and tailored to a particular audience. Internally, law enforcement agencies have also addressed the ongoing issue of lost evidence, focusing on making information secure but also widely accessible.

All of law enforcement recognizes a responsibility to counter hackers. To this extent, a growing number of state governments are creating multiagency groups to tackle cybersecurity. Cyber Threat Response is a forerunner; as alliance it includes the FBI, the Department of Homeland Security, and law enforcement agencies (Newcombe, 2016).

RECOMMENDATION

Law enforcement should utilize the same records management system. Information sharing has local, state, and national benefits for law enforcement agencies within the state of Texas. Shared information and collaborative activity would bridge the gap between law enforcement agencies. Conducting routine cross-training between agencies would also benefit the law enforcement community. Sharing the cloud system would also enforce the agencies' collaboration and improve law enforcement itself, at a reasonable cost during this era of shrinking budgets.

With the arrests of so many officers making newspaper headlines—although the percentage of arrests is low—agencies do have the right to act on their concern and not share information. This hesitation remains one of the biggest hindrances to universal adoption of the cloud system. Law enforcement agencies have made great strides in addressing those concerns and in actively reducing the number of systems being hacked, through public awareness campaigns and direct arrest and prosecution of cybercriminals. The key is, ultimately, to find the combination of words, tools, and actions that will move citizens and law enforcement into stronger collaborative relationships.

In closing, the benefits of shared information is invaluable to the Law Enforcement community. The Law Enforcement community should and would see the immediate impact of adopting this philosophy of information sharing. Law Enforcement agencies would work closer together creating a closer net- working within Law Enforcement. With the understanding all Law Enforcement agencies whether local, state and federal all could learn from one another.

Just as there are benefits, Law Enforcement agencies have to understand there is also a risk of adopting this philosophy. Certain personnel are privileged to access this shared information, making sure the boundaries are in place for sensitive information to be viewed. Law Enforcement agencies have to be careful not to have biases toward other agencies. Adopting the shared information is worth the risk for Law Enforcement agencies. Law Enforcement agencies should learn from mistakes of the past, adjusting the focus and becoming a world leading Law Enforcement community.

REFERENCES

9/11 Commission. (2004, July 22). *The final report of the National Commission on Terrorist Attacks upon the United States.* Retrieved from https://www.govinfo.gov/app/details/GPO-911REPORT/context.

Bertrand, N. (2015, June 25). *Former Baltimore cop reveals examples of police misconduct and corruption.* Retrieved from https://www.businessinsider.com/former-baltimore-cop-tweets-examples-of-police-misconduct-and-corruption-2015-6.

Bransford, S. D. (2012). An examination of factors affecting information sharing among law enforcement agencies (Doctoral dissertation).

Bune, Karen L. (2014, February 7) Dispatchers: Unsung heroes and a 'lifeline' for LEOs. *PoliceOne.* Retrieved from https://www.policeone.com/communications/articles/6815361-Dispatchers-Unsung-heroes-and-a-lifeline-for-LEOs/.

City of Stafford, Texas. (2016, September 29). *2016-2017 city budget.* Retrieved from http://www.staffordtx.gov/documents/budgets/2016-2017-city-budget.pdf.

Cybercrime and Punishment. (2014, September 2). *Infosecurity.* Retrieved from https://www.infosecurity-magazine.com/magazine-features/cybercrime-and-punishment/.

Ferrell, D. & Malnic, E. (1994, June 18). LAPD criticized for leniency in handling case. *Los Angeles Times.* Retrieved from http://articles.latimes.com/1994-06-18/news/mn-5398_1_murder-case

Garrett, R. (2008, October). Who You Gonna Call? *Law Enforcement Technology, 15*(10), 12-19.

Grewe, B. A. (2004, August 20). *Legal barriers to information sharing: The erection of a wall between intelligence and law enforcement investigations*. Retrieved from https://fas.org/irp/eprint/wall.pdf.

Jackman, T. (2016, June 22). *Study finds police officers arrested 1,100 times per year, or 3 per day, nationwide*. Retrieved from https://www.washingtonpost.com/news/true-crime/wp/2016/06/22/study-finds-1100-police-officers-per-year-or-3-per-day-are-arrested-nationwide/?utm_term=.3f019ed777cc

Kadifa, M. (2017, November 10). Drug sting nabs HPD officer. *Houston Chronicle,* Retrieved from http://www.houstonchronicle.com/news/houston-texas/houston/article/Drug-sting-nabs-HPD-officer-12349376.php.

Marshall, P. (2011, November 29). *Digital dragnet: How data became a cop's best weapon.* Retrieved from https://gcn.com/articles/2011/12/05/predictive-policing-tech-feature.aspx.

Mitchell, R. L. (2008, May 28). Criminal negligence: The state of law enforcement data sharing. *Computerworld.* Retrieved from https://www.cio.com/article/2436044/data-management/criminal-negligence--the-state-of-law-enforcement-data-sharing.html.

Murphy, D. (2015, April 9). Houston cop busted on drug charges with the brother of a Los Angeles cartel boss: Documents, *Houston Daily News.* Retrieved from https://www.nydailynews.com/news/national/houston-charged-conspiracy-tied-cartel-documents-article-1.2179875.

National Criminal Justice Association Initiative. (2004). *Justice Information Sharing*. Retrieved from https://www.ncja.org/ncja/policy/justice-information-sharing.

Newcombe, T. (2014, September 23). Cloud computing: Nearly ready for prime-time policing. *Government Technology*. Retrieved from http://www.govtech.com/public-safety/Cloud-Computing-Nearly-Ready-for-Prime-Time-Policing.html.

Nine indicted on gun trafficking and weapons charges as a result of historic partnership of AG's office, state police & ATF. (2010, May 27). *Official Web Site for the State of New Jersey.* Retrieved from http://www.nj.gov/oag/newsreleases10/pr20100527a.html

Kshemendra, P. (2013, November 19). Information sharing: Applying what we've learned since 9/11. *Information Week.* Retrieved from https://www.informationweek.com/information-sharing-applying-what-weve-learned-since-9-11-/d/d-id/899734

Petty, K. Protecting children from cybercrime: The twentieth session of the UN Commission on Crime Prevention and Criminal Justice. (2011, September). *Insights, 15*(24).

Romney, L. (2013, January 1). Cross-training of public safety workers attracting more interest. *Los Angeles Times*.

Reaves, B. A. (2011, July). Census of State and Local Law Enforcement Agencies.

Washington, DC: US Department of Justice.

Rutledge, G. & Inserra, D. (2017, April 12). 16 years after 9/11, gaps in information sharing still plague law enforcement. Daily Signal. Retrieved from https://www.dailysignal.com/2017/04/12/16-years-after-911-gaps-in-information-sharing-still-plague-law-enforcement-community/.

Sanders, T (2010, January) Law Enforcement Information Sharing and the Implications for Local Government. https://www.digitalcommunities.com

Sasko, C. (2016, June 7). Philly police officer charged with attempted extortion. *Philadelphia Magazine.* https://www.phillymag.com/news/2016/06/07/philadelphia-narcotics-officer-attempted-extortion/.

Schneier, B. (2009, November 12). FBI/CIA/NSA information sharing before 9/11, *Schneier on Security.* Retrieved from https://www.schneier.com/blog/archives/2009/11/fbiciansa_infor.html.

Forbes Technology Council. (2018, January 10). *Seven important steps law enforcement and government agencies can take to combat hackers.* Retrieved from https://www.forbes.com/sites/forbestechcouncil/2018/01/10/seven-important-steps-law-enforcement-and-government-agencies-can-take-to-combat-hackers/#5f25924a1759.

Shinder, D. (2011, January 26). What makes cybercrime laws so difficult to enforce. *TechRepublic.* Retrieved from https://www.techrepublic.com/blog/it-security/what-makes-cybercrime-laws-so-difficult-to-enforce/.

Sicart, M. (2009). *The ethics of computer games.* Cambridge, MA: MIT Press, 2009.

Smith, B. B. (n.d.). Avoiding the us vs. them mentality. *PoliceLink.* Retrieved from http://policelink.monster.com/education/articles/88372-avoiding-the-us-vs-them-mentality.

Stinson, P. M., Liederbach, J., Lab, S. P., & Brewer Jr., S. L. (2015). *Police integrity lost: A study of law enforcement officers arrested.* Washington: U.S. Department of Justice.

Stuart, B. A. & Taylor, E. J. (2017, August 23). The effect of social connectedness on crime: Evidence from the great migration. *Institute of Labor Economics,* Retrieved from http://conference.iza.org/conference_files/WoLabConf_2018/stuart_b26313.pdf.

Thorp, C. (2016, June 15). Police: Killeen police officer indicted on sexual assault charge*. Killeen Daily Herald.* Retrieved from http://kdhnews.com/news/crime/police-killeen-police-officer-indicted-on-sexual-assault-charge/article_24ea1314-3345-11e6-bbc2-77707c473d49.html.

Trend Micro. (2014, October 27). Major security, law enforcement groups team up to fight cybercrime. *Trend Micro.* Retrieved from https://blog.trendmicro.com/major-security-law-enforcement-groups-team-fight-cybercrime/.

U.S. Department of Justice, Bureau of Justice Assistance (2016, October). *Public safety primer on cloud technology.* Retrieved from https://it.ojp.gov/GIST/1195/File/FINAL%20Public%20Safety%20Primer%20On%20Cloud%20Technology.pdf.

Velez-Villar, E. (2012, February 28). *Statement before the House Homeland Security Committee, Subcommittee on Counterterrorism and Intelligence.* Retrieved from https://www.fbi.gov/news/testimony/intelligence-sharing-with-federal-state-and-local-law-enforcement-10-years-after-9-11.

Willis, D. S. (2010, December 1). Focus on training: The practice of spirituality and emotional wellness in law enforcement. *Department of Justice.* Retrieved from https://leb.fbi.gov/articles/focus/focus-on-training-the-practice-of-spirituality-and-emotional-wellness-in-law-enforcement.

Wyllie, D. (2009, April 30). Technology isn't the (biggest) problem for information sharing in law enforcement. *PoliceOne.* Retrieved from http://policelink.monster.com/education/articles/88372-avoiding-the-us-vs-them-mentality.

Young, D. (2013, July 1). Why are we pushing so hard on using the cloud for your data services? *United Public Safety* Retrieved from https://www.upsafety.net/docs/Why-are-we-pushing-so-hard-on-using-the-cloud-for-your-data-services.pdf.

Zukewich, M. P. (2004). Enhancing undercover police training (Master's thesis).